DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 170 and 171

RIN 0955–AA01

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Proposed rule.

SUMMARY: This proposed rule would implement certain provisions of the 21st Century Cures Act, including conditions and maintenance of certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program), the voluntary certification of health IT for use by pediatric health care providers, and reasonable and necessary activities that do not constitute information blocking. The implementation of these provisions would advance interoperability and support the access, exchange, and use of electronic health information. The proposed rule would also modify the 2015 Edition health IT certification criteria and Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

DATES: To be assured consideration, written or electronic comments must be received at one of the addresses provided below, no later than 5 p.m. on May 3, 2019.

ADDRESSES: You may submit comments, identified by RIN 0955–AA01, by any of the following methods (please do not submit duplicate comments). Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

- *Federal eRulemaking Portal:* Follow the instructions for submitting comments. Attachments should be in Microsoft Word, Microsoft Excel, or Adobe PDF; however, we prefer Microsoft Word. *http://www.regulations.gov.*
- *Regular, Express, or Overnight Mail:* Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Attention: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201. Please submit one original and two copies.
- *Hand Delivery or Courier:* Office of the National Coordinator for Health Information Technology, Attention: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Mary E. Switzer Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Enhancing the Public Comment Experience: To facilitate public comment on this proposed rule, a copy will be made available in Microsoft Word format on ONC's website (*http://www.healthit.gov*). We believe this version will make it easier for commenters to access and copy portions of the proposed rule for use in their individual comments. Additionally, a separate document (''public comment template'') will also be made available on ONC's website (*http://www.healthit.gov*) for the public to use in providing comments on the proposed rule. This document is meant to provide the public with a simple and organized way to submit comments on proposals and respond to specific questions posed in the preamble of the proposed rule. While use of this document is entirely voluntary, we encourage commenters to consider using the document in lieu of unstructured comments, or to use it as an addendum to narrative cover pages. We believe that use of the document may facilitate our review and understanding of the comments received. The public comment template will be available shortly after the proposed rule publishes in the **Federal Register**. This short delay will permit the appropriate citation in the public comment template to pages of the published version of the proposed rule.

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. Please do not include anything in your comment submission that you do not wish to share with the general public. Such information includes, but is not limited to: A person's social security number; date of birth; driver's license number; state identification number or foreign country equivalent; passport number; financial account number; credit or debit card number; any personal health information; or any business information that could be considered proprietary. We will post all comments that are received before the close of the comment period at *http://www.regulations.gov.*

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201 (call ahead to the contact listed below to arrange for inspection).

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Executive Summary

A. Purpose of Regulatory Action

ONC is responsible for the implementation of key provisions in Title IV of the 21st Century Cures Act (Cures Act) that are designed to advance interoperability; support the access, exchange, and use of electronic health information; and address occurrences of information blocking. This proposed rule would implement certain provisions of the Cures Act, including Conditions and Maintenance of Certification requirements for health information technology (health IT) developers, the voluntary certification of health IT for use by pediatric health providers, and reasonable and necessary activities that do not constitute information blocking. In addition, the proposed rule would implement parts of section 4006(a) of the Cures Act to support patient access to their electronic health information (EHI), such as making a patient's EHI more electronically accessible through the adoption of standards and certification criteria and the implementation of information blocking policies that support patient electronic access to their health information at no cost. Additionally, the proposed rule would modify the 2015 Edition health IT certification criteria and ONC Health IT Certification Program (Program) in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

In addition to fulfilling the Cures Act's requirements, the proposed rule would contribute to fulfilling Executive Order (E.O.) 13813. The President issued E.O. 13813 on October 12, 2017, to promote health care choice and competition across the United States. Section 1(c) of the E.O., in relevant part, states that government rules affecting the United States health care system should re-inject competition into the health care markets by lowering barriers to entry and preventing abuses of market power. Section 1(c) also states that government rules should improve access to and the quality of information that Americans need to make informed health care decisions. For example, as mentioned above, the proposed rule focuses on establishing Application Programming Interfaces (APIs) for several interoperability purposes, including patient access to their health information without special effort. The API approach also supports health care providers having the sole authority and autonomy to unilaterally permit connections to their health IT through certified API technology the health care providers have acquired. In addition, the proposed rule provides ONC's interpretation of the information blocking definition as established in the Cures Act and the application of the information blocking provision by identifying reasonable and necessary activities that would not constitute information blocking. Many of these activities focus on improving patient and health care provider access to electronic health information and promoting competition.

B. Summary of Major Provisions and Clarifications

1. Deregulatory Actions for Previous Rulemakings

Since the inception of the Program, we have aimed to implement and administer the Program in the least burdensome manner that supports our policy goals. Throughout the years, we have worked to improve the Program with a focus on ways to reduce burden, offer flexibility to both developers and providers, and support innovation. This approach has been consistent with the principles of Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), which instructs agencies to ''determine whether any [agency] regulations should be modified, streamlined, expanded, or repealed so as to make the agency's regulatory program more effective or less burdensome in achieving the regulatory objectives.'' To that end, we have historically, where feasible and appropriate, taken measures to reduce burden within the Program and make the Program more effective, flexible, and streamlined.

ONC has reviewed and evaluated existing regulations to identify ways to administratively reduce burden and implement deregulatory actions through guidance. In this proposed rule, we also propose potential new deregulatory actions that will reduce burden for health IT developers, providers, and other stakeholders. We propose six deregulatory actions in section III.B: (1) Removal of a threshold requirement related to randomized surveillance which allows ONC-Authorized Certification Bodies (ONC–ACBs) more flexibility to identify the right approach for surveillance actions, (2) removal of the 2014 Edition from the Code of Federal Regulations (CFR), (3) removal of the ONC-Approved Accreditor (ONC–AA) from the Program, (4) removal of certain 2015 Edition certification criteria, (5) removal of certain Program requirements, and (6) recognition of relevant Food and Drug Administration certification processes with a request for comment on the potential development of new processes for the Program.

2. Updates to the 2015 Edition Certification Criteria

This rule proposes to update the 2015 Edition by not only proposing criteria for removal, but by proposing to revise and add new certification criteria that would establish the capabilities and related standards and implementation specifications for the certification of health IT.

a. Adoption of the United States Core Data for Interoperability (USCDI) as a Standard

As part of ONC's continued efforts to assure the availability of a minimum baseline of data classes that could be commonly available for interoperable exchange, we adopted the 2015 Edition ''Common Clinical Data Set'' (CCDS) definition and used the CCDS shorthand in several certification criteria. However, the CCDS definition also began to be colloquially used for many different purposes. As the CCDS definition's relevance grew outside of its regulatory context, it became a symbolic and practical limit to the industry's collective interests to go beyond the CCDS data for access, exchange, and use. In addition, as we move further towards value-based care, the need for the inclusion of additional data classes that go beyond clinical data is necessary. In order to advance interoperability, we propose to remove the CCDS definition and its references from the 2015 Edition and replace it with the ''United States Core Data for Interoperability.'' We propose to adopt the USCDI as a standard, naming USCDI Version 1 (USCDI v1) in § 170.213 and incorporating it by reference in § 170.299. The USCDI standard, if adopted, would establish a set of data classes and constituent data elements that would be required to be exchanged in support of interoperability nationwide. To achieve the goals set forth in the Cures Act, ONC intends to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. Once the USCDI is adopted in regulation naming USCDI v1, health IT developers would be allowed to take advantage of a flexibility under the Maintenance of Certification real world testing requirements, which we refer to as the ''Standards Version Advancement Process'' (described in section VII.B.5 of this proposed rule). The Standards Version Advancement Process would permit health IT developers to voluntarily implement and use a new version of an adopted standard, such as the USCDI, so long as the newer version was approved by the National Coordinator through the Standards Version Advancement Process for use in certification.

b. Electronic Prescribing

We propose to update the electronic prescribing (e-Rx) SCRIPT standard in 45 CFR 170.205(b) to NCPDP SCRIPT 2017071, which would result in a new e-Rx standard eventually becoming the baseline for certification. We also propose to adopt a new certification criterion in § 170.315(b)(11) for e-Rx to reflect these updated proposals. ONC and CMS have historically maintained complementary policies of maintaining aligned e-Rx and medical history (MH) standards to ensure that the current standard for certification to the electronic prescribing criterion permits use of the current Part D e-Rx and MH standards. This proposal is made to ensure such alignment as CMS recently finalized its Part D standards to NCPDP SCRIPT 2017071 for e-RX and MH, effective January 1, 2020 (83 FR 16440). In addition to continuing to reference the current transactions included in § 170.315(b)(3), in keeping with CMS' final rule, we also propose to require all of the NCPDP SCRIPT 2017071 standard transactions CMS adopted at 42 CFR 423.160(b)(2)(iv).

c. Clinical Quality Measures—Report

We propose to remove the HL7 Quality Reporting Document Architecture (QRDA) standard requirements from the 2015 Edition ''CQMs—report'' criterion in § 170.315(c)(3) and, in their place, require Health IT Modules to support the CMS QRDA Implementation Guide (IGs).[1] This would reduce the burden for health IT developers by only having to support one form of the QRDA standard rather than two forms (*i.e.,* the HL7 and CMS forms).

d. Electronic Health Information Export

We propose a new 2015 Edition certification criterion for ''electronic health information (EHI) export'' in § 170.315(b)(10), which would replace the 2015 Edition ''data export'' certification criterion (§ 170.315(b)(6)) and become part of the 2015 Edition Base EHR definition. The proposed criterion supports situations in which we believe that all EHI produced and electronically managed by a developer's health IT should be made readily available for export as a standard capability of certified health IT. Specifically, this criterion would: (1) Enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient's behalf, and (2) support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system. This criterion would also require that the export include the data format, made publicly available, to facilitate the receiving health IT system's interpretation and use of the EHI to the extent reasonably practicable using the developer's existing technology.

This criterion provides developers with the ability to create innovative export capabilities according to their systems and data practices. We do not propose that the export must be executed according to any particular standard, but propose to require that the export must be accompanied by the data format, including its structure and syntax, to facilitate interpretation of the EHI therein. Overall, this new criterion is intended to provide patients and health IT users, including providers, a means to efficiently export the entire electronic health record for a single patient or all patients in a computable, electronic format.

e. Application Programming Interfaces (APIs)

We propose to adopt a new API criterion in § 170.315(g)(10), which would replace the ''application access—data category request'' certification criterion (§ 170.315(g)(8)) and become part of the 2015 Edition Base EHR definition. This new ''standardized API for patient and population services'' certification criterion would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards[2] and several implementation specifications. The new criterion would focus on supporting two types of API-enabled services: (1) Services for which a single patient's data is the focus and (2) services for which multiple patients' data are the focus.

f. Privacy and Security Transparency Attestations

We propose to adopt two new privacy and security transparency attestation certification criteria, which would identify whether certified health IT supports encrypting authentication credentials and/or multi-factor authentication. In order to be issued a certification, we propose to require that a Health IT Module developer attest to whether the Health IT Module encrypts authentication credentials and whether the Health IT Module supports multi-factor authentication. These criteria are not expected to place additional burden on health IT developers since they do not require net new development or implementation to take place in order to be met. However, certification to these proposed criteria would provide increased transparency and potentially motivate health IT developers to encrypt authentication credentials and support multi- factor authentication, which could help prevent exposure to unauthorized persons/entities.

g. Data Segmentation for Privacy and Consent Management

In the 2015 Edition, we adopted two ''data segmentation for privacy'' (DS4P) certification criteria, one for creating a summary record according to the DS4P standard and one for receiving a summary record according to the DS4P standard. Certification to the 2015 Edition DS4P criteria focus on data segmentation only at the document level. As noted in the 2015 Edition final rule (80 FR 62646)—and to our knowledge still an accurate assessment—certification to these criteria is currently not required to meet the Certified EHR Technology definition

[1] *https://ecqi.healthit.gov/qrda-quality-reporting-document-architecture.*

[2] *https://www.hl7.org/fhir/overview.html.*

(CEHRT) or required by any other HHS program. Since the 2015 Edition final rule, the health care industry has engaged in additional field testing and implementation of the DS4P standard. In addition, stakeholders shared with ONC—through public forums, listening sessions, and correspondence—that focusing certification on segmentation to only the document level does not permit providers the flexibility to address more granular segmentation needs. Therefore, we propose to remove the current 2015 Edition DS4P criteria. We propose to replace these two criteria with three new 2015 Edition ''DS4P'' certification criteria (two for C–CDA and one for a FHIR-based API) that would support a more granular approach to privacy tagging data consent management for health information exchange supported by either the C–CDA- or FHIR-based exchange standards.

3. Modifications to the ONC Health IT Certification Program

We propose to make corrections to the 2015 Edition privacy and security certification framework (80 FR 62705) and relevant regulatory provisions. These corrections have already been incorporated in the relevant Certification Companion Guides (CCGs).

We propose new and revised principles of proper conduct (PoPC) for ONC-Authorized Certification Bodies (ONC–ACBs). We propose to clarify that the records retention provision includes the ''life of the edition'' as well as after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules. We also propose to revise the PoPC in § 170.523(h) to clarify the basis for certification, including to permit a certification decision to be based on an evaluation conducted by the ONC–ACB for Health IT Modules' compliance with certification criteria by use of conformity methods approved by the National Coordinator for Health Information Technology (National Coordinator). We also propose to update § 170.523(h) to require ONC–ACBs to accept test results from any ONC–ATL that is in good standing under the Program and is compliant with its ISO 17025 accreditation requirements. We believe these proposed new and revised PoPCs would provide necessary clarifications for ONC–ACBs and would promote stability among the ONC–ACBs. We also propose to update § 170.523(k) to broaden the requirements beyond just the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (now renamed the Promoting Interoperability Programs) and provide other necessary clarifications.

We propose to revise a PoPC for ONC–ATLs. We propose to clarify that the records retention provision includes the ''life of the edition'' as well as after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules.

4. Health IT for the Care Continuum

Section 4001(b) of the Cures Act includes two provisions related to supporting health IT across the care continuum. The first instructs the National Coordinator to encourage, keep or recognize through existing authorities, the voluntary certification of health IT for use in medical specialties and sites of service where more technological advancement or integration is needed. The second outlines a provision related to the voluntary certification of health IT for use by pediatric health providers to support the health care of children. These provisions align closely with ONC's core purpose to promote interoperability to support care coordination, patient engagement, and health care quality improvement initiatives. Advancing health IT that promotes and supports patient care when and where it is needed continues to be a primary goal of the Program. This means health IT should support patient populations, specialized care, transitions of care, and practice settings across the care continuum.

ONC has explored how we might work with the health IT industry and with specialty organizations to collaboratively develop and promote health IT that supports medical specialties and sites of service. Over time, ONC has taken steps to make the Program modular, more open and accessible to different types of health IT, and able to advance functionality that is generally applicable to a variety of care and practice settings. Specific to the provisions in the Cures Act to support providers of health care for children, we considered a wide range of factors. These include: The evolution of health IT across the care continuum, the costs and benefits associated with health IT, the potential regulatory burden and compliance timelines, and the need to help advance health IT that benefits multiple medical specialties and sites of service involved in the care of children. In consideration of these factors, and to advance implementation of Sections 4001(b) of the Cures Act specific to pediatric care, we held a listening session where stakeholders could share their clinical knowledge and technical expertise in pediatric care and pediatric sites of service. Through the information learned at this listening session and our analysis of the health IT landscape for pediatric settings, we have identified existing 2015 Edition criteria, as well as new and revised 2015 Edition criteria proposed in this rule, that we believe could benefit providers of pediatric care and pediatric settings. In this proposed rule, we seek comment on our analysis and the correlated certification criteria that we believe would support the health care of children.

We also recognize the significance of the opioid epidemic confronting our nation and the importance of helping to support the health IT needs of health care providers committed to preventing inappropriate access to prescription opioids and to providing safe, appropriate treatment. We believe health IT offers promising strategies to help assist medical specialties and sites of services impacted by the opioid epidemic. Therefore, we request public comment on how our existing Program requirements and the proposals in this rulemaking may support use cases related to Opioid Use Disorder (OUD) prevention and treatment and if there are additional areas that ONC should consider for effective implementation of health IT to help address OUD prevention and treatment.

5. Conditions and Maintenance of Certification

We propose to establish certain Conditions and Maintenance of Certification requirements for health IT developers based on the conditions and maintenance of certification requirements outlined in section 4002 of the Cures Act. We propose an approach whereby the Conditions and Maintenance of Certification express both initial requirements for health IT developers and their certified Health IT Module(s) as well as ongoing requirements that must be met by both health IT developers and their certified Health IT Module(s) under the Program. In this regard, we propose to implement the Cures Act Conditions of Certification with further specificity as it applies to the Program and propose to implement any accompanying Maintenance of Certification requirements as standalone requirements to ensure that not only are the Conditions of Certification met, but that they are continually being met through the Maintenance of Certification requirements. For ease of reference and to distinguish from other conditions, we propose to capitalize ''Conditions of Certification'' and ''Maintenance of Certification'' when referring to Conditions and Maintenance of Certification requirements established under the Cures Act.

Information Blocking

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, not take any action that constitutes information blocking as defined in section 3022(a) of the Public Health Service Act (PHSA). We propose to establish this information blocking Condition of Certification in § 170.401. The Condition of Certification would prohibit any health IT developer under the Program from taking any action that constitutes information blocking as defined by section 3022(a) of the PHSA and proposed in § 171.103.

Assurances

Section 3001(c)(5)(D)(ii) of the Cures Act requires that a health IT developer, as a Condition of Certification under the Program, provide assurances to the Secretary that, unless for legitimate purposes specified by the Secretary, the developer will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA, or any other action that may inhibit the appropriate exchange, access, and use of EHI. We propose to implement this provision through several Conditions of Certification and accompanying Maintenance requirements, which are set forth in proposed § 170.402. We also propose to establish more specific Conditions and Maintenance of Certification requirements to provide assurances that a health IT developer does not take any other action that may inhibit the appropriate exchange, access, and use of EHI. These proposed requirements serve to provide further clarity under the Program as to how health IT developers can provide such broad assurances with more specific actions.

Communications

As a Condition and Maintenance of Certification under the Program, the Cures Act requires that health IT developers do not prohibit or restrict communications about certain aspects of the performance of health IT and the developers' related business practices. We propose that developers will be permitted to impose certain kinds of limited prohibitions and restrictions that we believe strike a reasonable balance between the need to promote open communication about health IT and related developer business practices and the need to protect the legitimate interests of health IT developers and other entities. However, certain narrowly-defined types of communications—such as communications required by law, made to a government agency, or made to a defined category of safety organization—would receive ''unqualified protection,'' meaning that developers would be absolutely prohibited from imposing any prohibitions or restrictions on such protected communications.

We propose that to maintain compliance with this Condition of Certification, a health IT developer must not impose or enforce any contractual requirement or legal right that contravenes this Condition of Certification. Furthermore, we propose that if a health IT developer has contracts/agreements in existence that contravene this condition, the developer must notify all affected customers or other persons or entities that the prohibition or restriction will not be enforced by the health IT developer. Going forward, health IT developers would be required to amend their contracts/agreements to remove or make void the provisions that contravene this Condition of Certification within a reasonable period of time, but not later than two years from the effective date of a subsequent final rule for this proposed rule.

Application Programming Interfaces (APIs)

The Cures Act's API Condition of Certification includes several key phrases (including, for example, ''without special effort'') and requirements for health IT developers that indicate the Cures Act's focus on the technical requirements as well as the actions and practices of health IT developers in implementing the certified API. In section VII.B.4 of the preamble, we outline our proposals to implement the Cures Act's API Condition of Certification. These proposals include new standards, new implementation specifications, a new certification criterion, as well as detailed Conditions and Maintenance of Certification requirements.

Real World Testing

The Cures Act adds a new Condition and Maintenance of Certification requirement that health IT developers successfully test the real world use of the technology for interoperability in the type of setting in which such technology would be marketed. In this proposed rule, we outline what successful ''real world testing'' means for the purpose of this Condition of Certification, as well as proposed Maintenance requirements—including standards updates for widespread and continued interoperability.

We propose to limit the applicability of this Condition of Certification to health IT developers with Health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange specified in section VII.B.5. We propose Maintenance of Certification requirements that would require health IT developers to submit publicly available annual real world testing plans as well as annual real world testing results for certified health IT products focused on interoperability. We also propose a Maintenance of Certification flexibility we have named the Standards Version Advancement Process, under which health IT developers with health IT certified to the criteria specified for interoperability and data exchange would have the option to update their health IT to a more advanced version(s) of the standard(s) or implementation specification(s) included in the criteria once such versions are approved by the National Coordinator through the Standards Version Advancement Process for use in health IT certified under the Program. Similarly, we propose that health IT developers presenting new health IT for certification to one of the criteria specified in Section VII.B.5 would have the option to certify to a National Coordinator-approved more advanced version of the adopted standards or implementation specifications included in the criteria. We propose that health IT developers voluntarily opting to avail themselves of the Standards Version Advancement Process must address their planned and actual timelines for implementation and rollout of standards updates in their annual real world testing plans and real world testing results submissions. We also propose that health IT developers of products with existing certifications who plan to avail themselves of the Standards Version Advancement Process flexibility notify both their ONC–ACB and their affected customers of their intention and plans to update their certified health IT and its anticipated impact on their existing certified health IT and customers, specifically including but not limited to whether, and if so for how long, the health IT developer intends to continue to support the certificate for the health IT certified to the prior version of the standard.

We propose a new PoPC for ONC–ACBs that would require ONC–ACBs to review and confirm that applicable health IT developers submit real world testing plans and real world results in accordance with our proposals. Once completeness is confirmed, ONC–ACBs would upload the plans and results via hyperlinks to the Certified Health IT Product List (CHPL). We propose to revise the PoPC in § 170.523(m) to require ONC–ACBs to collect, no less than quarterly, all updates successfully made to standards in certified health IT pursuant to the developers having voluntarily opted to avail themselves of the Standards Version Advancement Process flexibility under the real world testing Condition of Certification. We propose in § 170.523(t), a new PoPC for ONC–ACBs requiring them to ensure that developers seeking to take advantage of the Standards Version Advancement Process flexibility in § 170.405(b)(5) comply with the applicable requirements.

Attestations

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, provide to the Secretary an attestation to all the Conditions of Certification specified in the Cures Act, except for the ''EHR reporting criteria submission'' Condition of Certification. We propose to implement the Cures Act ''attestations'' Condition of Certification in § 170.406. Health IT developers would attest twice a year to compliance with the Conditions and Maintenance of Certification requirements (except for the EHR reporting criteria requirement, which would be metrics reporting requirements separately implemented through a future rulemaking). The 6-month attestation period we propose in § 170.406(b)(2) would properly balance the need to support appropriate enforcement with the attestation burden placed on health IT developers. In this regard, the proposed rule includes provisions to make the process as simple and efficient for health IT developers as possible (*e.g.,* 14-day grace period, web-based form submissions, and attestation alert reminders).

We propose that attestations would be submitted to ONC–ACBs on behalf of ONC and the Secretary. We propose a new PoPC in § 170.523(q) that an ONC–ACB must review and submit the health IT developers' attestations to ONC. ONC would then make the attestations publicly available through the CHPL.

EHR Reporting Criteria Submission

The Cures Act specifies that health IT developers be required, as a Condition and Maintenance of Certification under the Program, to submit reporting criteria on certified health IT in accordance with the EHR reporting program established under section 3009A of the PHSA, as added by the Cures Act. We have not yet established an EHR reporting program. Once ONC establishes such program, we will undertake rulemaking to propose and implement the associated Condition and Maintenance of Certification requirement(s) for health IT developers.

Enforcement

Section 4002 of the Cures Act adds Program requirements aimed at addressing health IT developer actions and business practices through the Conditions and Maintenance of Certification requirements, which expands the current focus of the Program requirements beyond the certified health IT itself. Equally important, section 4002 also provides that the Secretary of HHS may encourage compliance with the Conditions and Maintenance of Certification requirements and take action to discourage noncompliance. We, therefore, propose a general enforcement approach to encourage consistent compliance with the requirements. The proposed rule outlines a corrective action process for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement has not been or is not being met by a health IT developer under the Program. We propose, with minor modifications, to utilize the processes previously established for ONC direct review of certified health IT and codified in §§ 170.580 and 170.581 for the enforcement of the Conditions and Maintenance of Certification requirements. Where noncompliance is identified, our first priority would be to work with the health IT developer to remedy the matter through a corrective action process. However, we propose that, under certain circumstances, ONC may ban a health IT developer from the Program or terminate the certification of one or more of its Health IT Modules.

6. Information Blocking

Section 4004 of the Cures Act added section 3022 of the PHSA (42 U.S.C. 300jj–52, ''the information blocking provision''), which defines conduct by health care providers, and health IT developers of certified health IT, exchanges, and networks that constitutes information blocking. Section 3022(a)(1) of the PHSA defines information blocking in broad terms, while section 3022(a)(3) authorizes and charges the Secretary to identify reasonable and necessary activities that do not constitute information blocking (section 3022(a)(3) of the PHSA).

We identify several reasonable and necessary activities as exceptions to the information blocking definition, each of which we propose would not constitute information blocking for purposes of section 3022(a)(1) of the PHSA. The exceptions would extend to certain activities that interfere with the access, exchange, or use of EHI but that may be reasonable and necessary if certain conditions are met.

In developing the proposed exceptions, we were guided by three overarching policy considerations. First, the exceptions would be limited to certain activities that clearly advance the aims of the information blocking provision; promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI, and protecting patient safety; and promoting competition and innovation in health IT and its use to provide health care services to consumers. Second, each exception is intended to address a significant risk that regulated individuals and entities (*i.e.,* health care providers, health IT developers of certified health IT, health information networks, and health information exchanges) will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking. Third, and last, each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt.

The seven proposed exceptions are set forth in section VIII.D below. The first three exceptions, set forth in VIII.D.1–D.3 address activities that are reasonable and necessary to promote public confidence in the use of health IT and the exchange of EHI. These exceptions are intended to protect patient safety; promote the privacy of EHI; and promote the security of EHI. The next three exceptions, set forth in VIII.D.4–D.6, address activities that are reasonable and necessary to promote competition and consumer welfare. These exceptions would allow for the recovery of costs reasonably incurred; excuse an actor from responding to requests that are infeasible; and permit the licensing of interoperability elements on reasonable and non-discriminatory terms. The last exception, set forth in VIII.D.7, addresses activities that are reasonable and necessary to promote the performance of health IT. This proposed exception recognizes that actors may make health IT temporarily unavailable for maintenance or improvements that benefit the overall performance and usability of health IT.

To qualify for any of these exceptions, we propose that an individual or entity would, for each relevant practice and at all relevant times, have to satisfy all of the applicable conditions of the exception. Additionally, we propose (in section VIII.C of this preamble) to define or interpret terms that are present in section 3022 of the PHSA (such as the types of individuals and entities covered by the information blocking provision). We also propose certain new terms and definitions that are necessary to implement the information blocking provisions. We propose to codify the proposed exceptions and other information blocking proposals in a new part of title 45 of the Code of Federal Regulations, part 171.

C. Costs and Benefits

Executive Orders 12866 on Regulatory Planning and Review (September 30, 1993) and 13563 on Improving Regulation and Regulatory Review (February 2, 2011) direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). OMB has determined that this proposed rule is an economically significant rule as the potential costs associated with this proposed rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this proposed rule.

We have estimated the potential monetary costs and benefits of this proposed rule for health IT developers, health care providers, patients, ONC–ACBs, ONC–ATLs, and the federal government (*i.e.,* ONC), and have broken those costs and benefits out into the following categories: (1) Deregulatory actions (no associated costs); (2) updates to the updates to the 2015 Edition health IT certification criteria; (3) Conditions and Maintenance of Certification for a health IT developer; (4) oversight for the Conditions and Maintenance of Certification; and (5) information blocking.

We note that we have rounded all estimates to the nearest dollar and all estimates are expressed in 2016 dollars as it is the most recent data available to address all cost and benefit estimates consistently. We also note that we did not have adequate data to quantify some of the costs and benefits within this RIA. In those situations, we have described the qualitative costs and benefits of our proposals; however, such qualitative costs and benefits have not been accounted for in the monetary cost and benefit totals below.

We estimate that the total annual cost for this proposed rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would, on average, range from $365 million to $919 million with an average annual cost of $642 million. We estimate that the total perpetual cost for this proposed rule (starting in year two), based on the cost estimates outlined above, would, on average, range from $228 million to $452 million with an average annual cost of $340 million.

We estimate the total annual benefit for this proposed rule would range from $3.08 billion to $9.15 billion with an average annual benefit of $6.1 billion.

We estimate the total annual net benefit for this proposed rule for the first year after it is finalized (including one-time costs), based on the cost and benefit estimates outlined above, would range from $2.7 billion to $8.2 billion with an average net benefit of $5.5 billion. We estimate the total perpetual annual net benefit for this proposed rule (starting in year two), based on the cost-benefit estimates outlined above, would range from $2.9 billion to $8.7 billion with an average net benefit of $5.8 billion.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the Recovery Act) (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created ‘‘Title XXX—Health Information Technology and Quality’’ (Title XXX) to improve health care quality, safety, and efficiency through the promotion of health IT and electronic health information (EHI) exchange.

The Cures Act was enacted on December 13, 2016, to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes. The Cures Act, through Title IV—Delivery, amended the HITECH Act (Title XIII of Division A of Pub. L. 111–5) by modifying or adding certain provisions to the PHSA relating to health IT.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two new federal advisory committees, the HIT Policy Committee (HITPC) and the HIT Standards Committee (HITSC). Each was responsible for advising the National Coordinator for Health Information Technology (National Coordinator) on different aspects of standards, implementation specifications, and certification criteria.

Section 3002 of the Cures Act amended the PHSA by replacing the HITPC and HITSC with one committee, the Health Information Technology Advisory Committee (HIT Advisory Committee or HITAC). Section 3002(a) establishes that the HITAC shall advise and recommend to the National Coordinator on different aspects of standards, implementation specifications, and certification criteria, relating to the implementation of a health IT infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information. Further described in section 3002(b)(1)(A) of the PHSA, this includes providing to the National Coordinator recommendations on a policy framework to advance interoperable health IT infrastructure, updating recommendations to the policy framework, and making new recommendations, as appropriate. Section 3002(b)(2)(A) identifies that in general, the HITAC shall recommend to the National Coordinator for purposes of adoption under section 3004, standards, implementation specifications, and certification criteria and an order of priority for the development, harmonization, and recognition of such standards, specifications, and certification criteria. Like the process previously required of the former HITPC and HITSC, the HITAC will develop a schedule for the assessment of policy recommendations for the Secretary to publish in the **Federal Register**.

Section 3004 of the PHSA identifies a process for the adoption of health IT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria. As specified in section 3004(a)(1), the Secretary is required, in consultation with representatives of other relevant federal agencies, to jointly review standards, implementation specifications, and certification criteria endorsed by the National Coordinator under section 3001(c) and subsequently determine whether to propose the adoption of any grouping of such standards, implementation specifications, or certification criteria. The Secretary is required to publish all determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA titled, Subsequent Standards Activity, provides that the Secretary shall adopt additional standards, implementation specifications, and certification criteria as necessary and consistent with the schedule published by the HITAC. We consider this provision in the broader context of the HITECH Act and Cures Act to grant the Secretary the authority and discretion to adopt standards, implementation specifications, and certification criteria that have been recommended by the HITAC and endorsed by the National Coordinator, as well as other appropriate and necessary health IT standards, implementation specifications, and certification criteria.

2. Health IT Certification Program(s)

Under the HITECH Act, section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Specifically, section 3001(c)(5)(A) specifies that the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), shall keep or recognize a program or programs for the voluntary certification of health IT that is in compliance with applicable certification criteria adopted under this subtitle (*i.e.,* certification criteria adopted by the Secretary under section 3004 of the PHSA). The certification program(s) must also include, as appropriate, testing of the technology in accordance with section 13201(b) of the HITECH Act. Overall, section 13201(b) of the HITECH Act requires that with respect to the development of standards and implementation specifications, the Director of NIST shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. The HITECH Act also indicates that the development of this conformance testing infrastructure may include a program to accredit independent, non-federal laboratories to perform testing.

Section 3001(c)(5) of the PHSA was amended by the Cures Act, which instructs the National Coordinator to encourage, keep, or recognize, through existing authorities, the voluntary certification of health IT under the Program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. Section 3001(c)(5)(C)(iii) identifies that the Secretary, in consultation with relevant stakeholders, shall make recommendations for the voluntary certification of health IT for use by pediatric health providers to support the care of children, as well as adopt certification criteria under section 3004 to support the voluntary certification of health IT for use by pediatric health providers. The Cures Act further amended section 3001(c)(5) of the PHSA by adding section 3001(c)(5)(D), which provides the Secretary with the authority, through notice and comment rulemaking, to require conditions and maintenance of certification requirements for the Program.

B. Regulatory History

The Secretary issued an interim final rule with request for comments (75 FR 2014, Jan. 13, 2010), which adopted an initial set of standards, implementation specifications, and certification criteria. On March 10, 2010, ONC published a proposed rule (75 FR 11328) that proposed both a temporary and permanent certification program for the purposes of testing and certifying health IT. A final rule establishing the temporary certification program was published on June 24, 2010 (75 FR 36158) and a final rule establishing the permanent certification program was published on January 7, 2011 (76 FR 1262). ONC issued multiple rulemakings since these initial rulemaking to update standards, implementation specifications, and certification criteria and the certification program, a history of which can be found in the final rule titled, ''2015 Edition Health Information (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications'' (Oct. 16, 2015, 80 FR 62602) (''2015 Edition final rule''). A correction notice was published for the 2015 Edition final rule on December 11, 2015 (80 FR 76868) to correct preamble and regulatory text errors and clarify requirements of the Common Clinical Data Set (CCDS), the 2015 Edition privacy and security certification framework, and the mandatory disclosures for health IT developers.

The 2015 Edition final rule established a new edition of certification criteria (''2015 Edition health IT certification criteria'' or ''2015 Edition'') and a new 2015 Edition Base EHR definition. The 2015 Edition established the capabilities and specified the related standards and implementation specifications that CEHRT would need to include to, at a minimum, support the achievement of ''meaningful use'' by eligible clinicians, eligible hospitals, and critical access hospitals under the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) (now referred to as the Promoting Interoperability Programs)[3] when the 2015 Edition is required for use under these and other programs referencing the CEHRT definition. The 2015 Edition final rule also made changes to the Program. The final rule adopted a proposal to change the Program's name to the ''ONC Health IT Certification Program'' from the ONC *HIT* Certification Program, modified the Program to make it more accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond the ambulatory and inpatient settings, and adopted new and revised Principles of Proper Conduct (PoPC) for ONC–ACBs.

After issuing a proposed rule on March 2, 2016 (81 FR 11056), ONC published a final rule titled, ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' (81 FR 72404) (''EOA final rule'') on October 19, 2016. The final rule finalized modifications and new requirements under the Program, including provisions related to ONC's role in the Program. The final rule created a regulatory framework for ONC's direct review of health IT certified under the Program, including, when necessary, requiring the correction of non-conformities found in health IT certified under the Program and suspending and terminating certifications issued to Complete EHRs and Health IT Modules. The final rule also sets forth processes for ONC to authorize and oversee accredited testing laboratories under the Program. In addition, it includes provisions for expanded public availability of certified health IT surveillance results.

III. Deregulatory Actions for Previous Rulemakings

A. Background

1. History of Burden Reduction and Flexibility

Since the inception of the ONC Health IT Certification Program (Program), we have aimed to implement and administer the Program in the least burdensome manner that supports our policy goals. Throughout the years, we

[3] *https://www.federalregister.gov/d/2018-16766/p-4.*

have worked to improve the Program with a focus on ways to reduce burden, offer flexibility to both developers and providers, and support innovation. This approach has been consistent with the principles of Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), which instructs agencies to ''determine whether any [agency] regulations should be modified, streamlined, expanded, or repealed so as to make the agency's regulatory program more effective or less burdensome in achieving the regulatory objectives.'' To that end, we have historically, where feasible and appropriate, taken measures to reduce burden within the Program and make the Program more effective, flexible, and streamlined.

For example, in the 2014 Edition final rule (77 FR 54164), we revised the certified electronic health record technology (CEHRT) definition to provide flexibility and create regulatory efficiencies by narrowing required functionality to a core set of capabilities (*i.e.,* the Base EHR definition) plus the additional capabilities each eligible clinician, eligible hospital, and critical access hospital needed to successfully achieve the applicable objective and measures under the EHR Incentive Programs (now referred to as the Promoting Interoperability Programs). ONC has also supported more efficient testing and certification methods and reduced regulatory burden through the adoption of a gap certification policy. As explained in the 2014 Edition final rule (77 FR 54254) and the 2015 Edition final rule (80 FR 62681), where applicable, gap certification allows for the use of a previously certified health IT product's test results to certification criteria identified as unchanged. Developers have been able to use gap certification for the more efficient certification of their health IT when updating from the 2011 Edition to the 2014 Edition and from the 2014 Edition to the 2015 Edition.

ONC introduced further means to reduce regulatory burden, increase regulatory flexibility, and promote innovation in the 2014 Edition Release 2 final rule (79 FR 54430). The 2014 Edition Release 2 final rule established a set of optional 2014 Edition certification criteria that provided flexibility and alternative certification pathways for health IT developers and providers based on their specific circumstances. The 2014 Edition Release 2 final rule also simplified the Program by discontinuing the use of the ''Complete EHR'' certification concept beginning with the 2015 Edition (79 FR 54443).

In the 2015 Edition final rule, we did not ''carry forward'' certain 2014 Edition certification criteria into the 2015 Edition, such as the ''image results,'' ''patient list creation,'' and ''electronic medication administration record'' criteria. We determined that these criteria did not advance functionality or support interoperability (80 FR 62682–84). We also did not require all health IT to be certified to the ''meaningful use measurement'' certification criteria for ''automated numerator recording'' and ''automated measure calculation'' (80 FR 62605), which had been previously required for the 2014 Edition. Based on stakeholder feedback and Program administration observations, we also permitted testing efficiencies for the 2015 Edition ''automated numerator recording'' and ''automated measure calculation'' criteria by removing the live demonstration requirement of recording data and generating reports. Health IT developers may now self-test their Health IT Modules(s) and submit the resulting reports to the ONC-Authorized Testing Laboratory (ONC–ATL) to verify compliance with the criterion.[4] In order to further reduce burden for health IT developers, we adopted a simpler, straight-forward approach to privacy and security certification requirements, which clarified which requirements are applicable to each criterion within the regulatory functional areas (80 FR 62605).

2. Executive Orders 13771 and 13777

On January 30, 2017, the President issued Executive Order 13771 on Reducing Regulation and Controlling Regulatory Costs, which requires agencies to identify deregulatory actions. This order was followed by Executive Order 13777, titled ''Enforcing the Regulatory Reform Agenda'' (February 24, 2017). Executive Order 13777 provides further direction on implementing regulatory reform by identifying a process by which agencies must review and evaluate existing regulations and make recommendations for repeal or simplification.

In order to implement these regulatory reform initiatives and policies, over the past year ONC reviewed and evaluated existing regulations. During our review, we sought to identify ways to further reduce administrative burden, to implement deregulatory actions through guidance, and to propose potential new deregulatory actions in this proposed rule that will reduce burden for health IT developer, providers, and other stakeholders.

On August 21, 2017, ONC issued *Relied Upon Software Program Guidance.*[5] Health IT developers are permitted to use ''relied upon software'' (76 FR 1276) to demonstrate compliance with certification criteria adopted at 45 CFR part 170, subpart C. Historically, in cases where a Health IT Module is paired with multiple ''relied upon software'' products for the same capability, health IT developers were required to demonstrate compliance for the same certification criterion with each of those ''relied upon software'' products in order for the products to be listed on the Certified Health IT Product List (CHPL). With the issued guidance, health IT developers may now demonstrate compliance with only one ''relied upon software'' product for a criterion/capability. Once the health IT developer demonstrates compliance with a minimum of one ''relied upon software'' product, the developer can have multiple, additional ''relied upon software'' products for the same criterion/capability listed on the CHPL (*https://chpl.healthit.gov/*). This approach reduces burden for health IT developers, ONC–ATLs, and ONC-Authorized Certification Bodies (ONC–ACBs).

On September 21, 2017, ONC reduced the overall burden for testing health IT to the 2015 Edition.[6] ONC reviewed the 2015 Edition test procedures, which identify minimum testing requirements ONC–ATLs must evaluate during testing. ONC changed 30 of the 2015 Edition test procedures to attestation only (*i.e.,* a ''yes'' self-declaration by the health IT developer that their product has capabilities conformant with those specified in the associated certification criterion/criteria).[7] This deregulatory action reduced burden and costs program-wide, while still maintaining the Program's high level of integrity and assurances. Health IT developers now have reduced preparation and testing costs for testing to these criteria. Specifically, the cost savings for health IT developers have been estimated between $8.34 and $9.26 million. ONC–ATLs also benefit by having more time and resources to focus on tool-based

[4] *https://www.healthit.gov/test-method/automated-numerator-recording* and *https://www.healthit.gov/test-method/automated-measure-calculation.*

[5] *https://www.healthit.gov/sites/default/files/relieduponsoftwareguidance.pdf.*

[6] *https://www.healthit.gov/buzz-blog/healthit-certification/certification-program-updates-support-efficiency-reduce-burden/.*

[7] *https://www.healthit.gov/sites/default/files/policy/selfdeclarationapproachprogramguidance17-04.pdf.*

testing (for interoperability-oriented criteria) and being responsive to any retesting requirements that may arise from ONC–ACB surveillance activities. Furthermore, providers and users of certified health IT do not lose confidence in the Program because this burden reduction effort in no way alters the expectations of conformance and responsibilities of Program participants. Health IT developers are still required to meet certification criteria requirements and maintain their products' conformance to the full scope of the associated criteria, including when implemented in the field and in production use. Similarly, ONC and ONC–ACBs continue to conduct surveillance activities and respond to end-user complaints.

B. Proposed Deregulatory Actions

We propose six deregulatory actions below. We welcome comments on these potential deregulatory actions and any other potential deregulatory actions we should consider. We also refer readers to section XIV (Regulatory Impact Analysis) of this proposed rule for a discussion of the estimated cost savings from these proposed deregulatory actions.

1. Removal of Randomized Surveillance Requirements

ONC–ACBs are required to conduct surveillance of certified health IT under the Program to ensure that health IT continues to conform and function as required by the full scope of the certification requirements. Surveillance is categorized as either reactive surveillance (for example, complaint-based surveillance) or randomized surveillance, which, by regulation, requires ONC–ACBs to proactively surveil 2% of the certificates they issue annually. On September 21, 2017, we exercised enforcement discretion with respect to the implementation of randomized surveillance by ONC–ACBs.[8] Consistent with this exercise of enforcement discretion, we now propose to eliminate certain regulatory randomized surveillance requirements.

We propose to revise § 170.556(c) by changing the requirement that ONC–ACBs *must* conduct in-the-field, randomized surveillance to specify that ONC–ACBs *may* conduct in-the- field, randomized surveillance. We further propose to remove § 170.556(c)(2), which specifies that ONC–ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year. We also propose to remove the requirements in § 170.556(c)(5) regarding the exclusion and exhaustion of selected locations for randomized surveillance. Additionally, we propose to remove the requirements in § 170.556(c)(6) regarding the consecutive selection of certified health IT for randomized surveillance. Without these regulatory requirements, ONC–ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, using the methodology identified by ONC with respect to scope (§ 170.556(c)(1)), selection method (§ 170.556(c)(3)), and the number and types of locations for in-the-field surveillance (§ 170.556(c)(4)).

Stakeholders have expressed concern that the benefits of in-the-field, randomized surveillance may not outweigh the time commitment required by providers, particularly if no non-conformities are found. In general, providers have expressed that reactive surveillance (*e.g.,* surveillance based on user complaints) is a more logical and economical approach to surveillance. The removal of randomized surveillance requirements would also give ONC–ACBs the flexibility and time to focus on other priorities, such as the certification of health IT to the 2015 Edition. Therefore, as discussed above, we propose to eliminate certain regulatory randomized surveillance requirements.

2. Removal of the 2014 Edition From the Code of Federal Regulations

We propose to remove the 2014 Edition from the Code of Federal Regulations (CFR). The 2014 Edition was the result of rulemaking completed in 2012 and includes standards and functionality that are now significantly outmoded. Removal of the 2014 Edition would make the 2015 Edition the baseline for health IT certification. The 2015 Edition, including the additional certification criteria, standards, and requirements proposed in this proposed rule, better enables interoperability and the access, exchange, and use of electronic health information. Adoption and implementation of the 2015 Edition, including the proposals in this proposed rule, would also lead to the benefits outlined in the 2015 Edition final rule (80 FR 62602–62603, 62605–62606, 62740) and in this proposed rule (*see, for example,* the Executive Summary and the ''Assurances,'' ''API'', and ''Real World Testing'' Conditions and Maintenance of Certification sections). Equally important, adoption and implementation of the 2015 Edition by providers would lead to the estimated costs savings in this proposed rule through improved interoperability supporting the access, exchange, and use of electronic health information.

Removal of the 2014 Edition would eliminate inconsistencies and costs caused by health IT certification and implementation of two different editions with different functionalities and versions of standards. Patient care could improve through the reduced risk of error that comes with the health care system's consistent implementation and use of health IT certified to the 2015 Edition. Innovation could also improve with health IT developers (including third-party software developers) developing to only one set of newer standards and implementation specifications, which would be more predictable and less costly.

Removal of the 2014 Edition would also reduce regulatory burden by no longer requiring the maintenance and support of the 2014 Edition. Maintaining compliance with only the 2015 Edition would reduce the cost and burden for health IT developers, ONC–ACBs, and ONC–ATLs because they would no longer have to support two increasingly distinct sets of requirements as is the case now with certification to both the 2014 and 2015 Editions. More specifically, health IT developers would not have to support two maintenance infrastructures and updating for their customers; nor would ONC–ATLs and ONC–ACBs have to support testing, certification, and surveillance for two separate editions of certified health IT.

As referenced by the HHS Office of Inspector General (OIG) and Centers for Medicare & Medicaid Services (CMS) in their rulemakings regarding donations of EHR items and services, we committed to retiring certification criteria editions that are no longer applicable.[9] We first did this with the removal of the 2011 Edition (79 FR 54447). Accordingly, our proposal to remove the outdated 2014 Edition for the reasons discussed above would also streamline Program compliance requirements and ensure there is no regulatory confusion between ONC's rules and other HHS rules.

To implement the removal of the 2014 Edition from the CFR, we propose to remove the 2014 Edition certification

[8] *https://www.healthit.gov/sites/default/files/ONC_Enforcement_Discretion_Randomized_Surveillance_8-30-17.pdf.*

[9] CMS final rule ''Medicare Program; Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships: Exception for Certain Electronic Health Records Arrangements'' (*78 FR 78751*).OIG final rule ''Medicare and State Health Care Programs: Fraud and Abuse; Electronic Health Records Safe Harbor Under the Anti-Kickback Statute'' (*78 FR 79202*).

criteria (§ 170.314) and related standards, terms, and requirements from the CFR. In regard to terms, we propose to retire the 2014 Edition-related definitions found in § 170.102, including the ''2014 Edition Base EHR,'' ''2014 Edition EHR certification criteria,'' and ''Complete EHR, 2014 Edition.'' As explained in the 2015 Edition final rule (80 FR 62719), the ability to maintain Complete EHR certification is only permitted with health IT certified to the 2014 Edition certification criteria. Because this concept was discontinued for the 2015 Edition, we propose to remove § 170.545 and any references to Complete EHR from the regulation text in conjunction with the removal of the 2014 Edition. We also propose to remove references to the 2014 Edition from the Common Clinical Data Set (CCDS) definition. However, as discussed later in section IV.B.1 (''United States Core Data for Interoperability'') of this proposed rule, we propose to remove the CCDS definition from the CFR and effectively replace it with a new government-unique standard, the United States Core Data for Interoperability (USCDI), proposing to adopt Version 1 (v1) in § 170.213. The new standard would be applicable to certain 2015 Edition certification criteria that currently reference the CCDS, subject to any of these criteria being removed through this rulemaking).

We propose to remove the standards and implementation specifications found in §§ 170.200, 170.202, 170.204, 170.205, 170.207, 170.210, and 170.299 that are only referenced in the 2014 Edition certification criteria. Adopted standards that are also referenced in the 2015 Edition would remain. We propose to remove requirements in § 170.550(f) and any other requirements in subpart E, §§ 170.500 through 170.599, which are specific to the 2014 Edition and do not apply to the 2015 Edition.

In order to avoid regulatory conflicts, we are taking into consideration the final rule released by CMS on November 2, 2017, which makes payment and policy changes to the second year of the Quality Payment Program (QPP). The CMS's final rule, titled ''Medicare Program; CY 2018 Updates to the Quality Payment Program: Extreme and Uncontrollable Circumstance Policy for the Transition Year'' (82 FR 53568), permits eligible clinicians to use health IT certified to either the 2014 or 2015 Edition certification criteria, or a combination of the two for the CY 2018 performance period. The QPP final rule also states that the 2015 Edition will be the sole edition permitted to meet the CEHRT definition starting with the CY 2019 program year.

Therefore, we propose that the effective date of removal of the 2014 Edition certification criteria and related standards, terms, and requirements from the CFR would be the effective date of a subsequent final rule for this proposed rule, which we expect will be issued in the latter half of 2019. We note that we will continue to support Medicare and Medicaid program attestations by maintaining an archive on the CHPL allowing the public to access historic information on a product certified to the 2014 Edition.

3. Removal of the ONC-Approved Accreditor From the Program

We propose to remove the ONC-Approved Accreditor (ONC–AA) from the Program. The ONC–AA's role is to accredit certification bodies for the Program and to oversee the ONC–ACBs. However, years of experience and changes with the Program have led ONC to conclude that, in many respects, the role of the ONC–AA to oversee ONC–ACBs is now duplicative of ONC's oversight. More specifically, ONC's experience with administering the Principles of Proper Conduct for ONC–ACBs as well as issuing necessary regulatory changes (*e.g.,* ONC–ACB surveillance and reporting requirements in the 2015 Edition final rule) has demonstrated that ONC on its own has the capacity to provide the appropriate oversight of ONC–ACBs. Therefore, we believe removal of the ONC–AA would reduce the Program's administrative complexity and burden.

To implement this proposed deregulatory action, we propose to remove the definition for ''ONC-Approved Accreditor or ONC–AA'' found in § 170.502. We also propose to remove processes related to ONC–AAs found in §§ 170.501(c), 170.503, and 170.504 regarding requests for ONC–AA status, ONC–AA ongoing responsibilities, and reconsideration for requests for ONC–AA status. Regarding correspondence and communication with ONC, we propose to remove specific references to the ''ONC–AA'' and ''accreditation organizations requesting ONC–AA status'' by revising § 170.505. We also propose to remove the final rule titled ''Permanent Certification Program for Health Information Technology; Revisions to ONC-Approved Accreditor Processes'' (76 FR 72636) which established a process for addressing instances where the ONC–AA engages in improper conduct or does not perform its responsibilities under the Program. Because this prior final rule relates solely to the role and removal of the ONC–AA, we propose its removal and § 170.575, which codified the final rule in the CFR.

These proposed deregulatory actions would also provide an additional benefit for ONC–ACBs. ONC–ACBs would be able to obtain and maintain accreditation to ISO/IEC 17065, with an appropriate scope, from any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF). Accordingly, we propose to revise the application process for ONC–ACB status in § 170.520(a)(3) to require documentation that confirms that the applicant has been accredited to ISO/IEC 17065, with an appropriate scope, by any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF), in place of the ONC–AA accreditation documentation requirements. Similarly, instead of requiring the ONC–AA to evaluate the conformance of ONC–ACBs to ISO/IEC 17065, we propose to revise § 170.523(a) to simply require ONC–ACBs to maintain accreditation in good standing to ISO/IEC 17065 for the Program. This means that ONC–ACBs would need to continue to comply with ISO/IEC 17065 and requirements specific to the ONC Health IT Certification Program scheme.

4. Removal of Certain 2015 Edition Certification Criteria and Standards

We have reviewed and analyzed the 2015 Edition to determine whether there are certification criteria we could remove. We have identified both criteria and standards for removal as proposed below. We believe the removal of these criteria and standards will reduce burden and costs for health IT developers and health care providers by eliminating the need to: Design and meet specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting and disclosure requirements; maintain and update certifications for certified functionalities; and participate in surveillance of certified health IT. To these points, if our proposals are finalized in a subsequent final rule, we would expect any already issued 2015 Edition certificates to be updated to reflect the removal of applicable 2015 Edition certification criteria. We welcome comment on the proposed removal of the identified criteria and standards below and any other 2015 Edition criteria and standards we should consider for removal.

a. 2015 Edition Base EHR Definition Criteria

We propose the removal of certain certification criteria from the 2015 Edition that are included in the 2015 Edition Base EHR definition. The removal of these criteria would support burden and cost reductions for health IT developers and health care providers as noted above.

i. Problem List

We propose to remove the 2015 Edition ''problem list'' certification criterion (§ 170.315(a)(6)). The functionality in this criterion was first adopted as a 2011 Edition certification criterion to support the associated meaningful use Stage 1 objective and measure for recording problem list information. In this regard, SNOMED CT® was adopted specifically to support the measure. This 2015 Edition ''problem list'' criterion remains relatively functionally the same as the 2011 Edition and has exactly the same functionally as the 2014 Edition ''problem list'' criterion.

We propose to remove this criterion for multiple reasons. First, this criterion no longer supports the ''recording'' objective and measure of the CMS Promoting Interoperability Programs as such objective and measure no longer exist. Second, the functionality is sufficiently widespread among health care providers since it has been part of certification and the Certified EHR Technology definition since the 2011 Edition and has not substantively changed with the 2015 Edition. Third, we do not believe this functionality would be removed from health IT systems because of our proposal to remove it from the 2015 Edition Base EHR definition. This functionality is essential to clinical care and would be in EHR systems absent certification, particularly considering the limited certification requirements. Fourth, this functionality does not directly support interoperability as the capabilities are focused on internally recording EHI. In this regard, representing problems with SNOMED CT® is part of the USCDI and, thus, better supports interoperability through its availability for access and exchange. Accordingly, we propose to remove the ''problem list'' criterion from the 2015 Edition, including the 2015 Edition Base EHR definition. We note that once removed from the 2015 Edition, the criterion would also no longer be included in the 2015 Edition ''safety-enhanced design'' criterion.

ii. Medication List

We propose to remove the 2015 Edition ''medication list'' certification criterion (§ 170.315(a)(7)). The functionality in this criterion was first adopted as a 2011 Edition certification criterion to support the associated meaningful use Stage 1 objective and measure for recording medication list information. The criterion does not require use of a vocabulary standard to record medications. This 2015 Edition ''medication list'' criterion remains functionally the same as the 2011 Edition and 2014 Edition ''medication list'' criteria.

We propose to remove this criterion for multiple reasons. First, this criterion no longer supports a ''recording'' objective and measure of the CMS Promoting Interoperability Programs as such objective and measure no longer exist. Second, the functionality is sufficiently widespread among health care providers since it has been part of certification and the Certified EHR Technology definition since the 2011 Edition and has not substantively changed with the 2015 Edition. Third, we do not believe this functionality would be removed from EHR systems because of our proposal to remove it from the 2015 Edition Base EHR definition. This functionality is essential to clinical care and would be in EHR systems absent certification, particularly considering the limited certification requirements. Fourth, this functionality does not directly support interoperability as the capabilities are focused on internally recording EHI. In this regard, this criterion does not even require representation of medications in standardized nomenclature. Fifth, medications are included in the USCDI and must be represented in RxNorm as part of the USCDI. This approach better supports interoperability through medication information being availability for access and exchange in a structured format. Accordingly, we propose to remove the ''medications list'' criterion from the 2015 Edition, including the 2015 Edition Base EHR definition. We note that once removed from the 2015 Edition, the criterion would also no longer be included in the 2015 Edition ''safety-enhanced design'' criterion.

iii. Medication Allergy List

We propose to remove the 2015 Edition ''medication allergy list'' certification criterion (§ 170.315(a)(8)). The functionality in this criterion was first adopted as a 2011 Edition certification criterion to support the associated meaningful use Stage 1 objective and measure for recording this information. The criterion does not require use of a vocabulary standard to record medication allergies. This 2015 Edition ''medication allergy list'' criterion remains functionally the same as the 2011 Edition and 2014 Edition ''medication allergy list'' criteria.

We propose to remove this criterion for multiple reasons. First, this criterion no longer supports a ''recording'' objective and measure of the CMS Promoting Interoperability Programs as such objective and measure no longer exist. Second, the functionality is sufficiently widespread among health care providers since it has been part of certification and the Certified EHR Technology definition since the 2011 Edition and has not substantively changed with the 2015 Edition. Third, we do not believe this functionality would be removed from EHR systems because of our proposal to remove it from the 2015 Edition Base EHR definition. This functionality is essential to clinical care and would be in EHR systems absent certification, particularly considering the limited certification requirements. Fourth, this functionality does not directly support interoperability as the capabilities are focused on internally recording EHI. In this regard, this criterion does not even require representation of medication allergies in standardized nomenclature. Fifth, medication allergies are included in the USCDI and must be represented in RxNorm as part of the USCDI. This approach better supports interoperability through medication allergy information being availability for access and exchange in a structured format. Accordingly, we propose to remove the ''medication allergy list'' criterion from the 2015 Edition, including the 2015 Edition Base EHR definition. We note that once removed from the 2015 Edition, the criterion would also no longer be included in the 2015 Edition ''safety- enhanced design'' criterion.

iv. Smoking Status

We propose to remove the 2015 Edition ''smoking status'' criterion (§ 170.315(a)(11)), which would include removing it from the 2015 Edition Base EHR definition. We previously adopted a 2015 Edition ''smoking status'' certification criterion that does not reference a standard. However, the CCDS definition requires smoking status to be coded in accordance with SNOMED CT®. While we continue to believe that the capture of a patient's smoking status has significant value in assisting providers with addressing the number one cause of preventable death and disease in the United States, we no longer believe that a criterion that simply ensures this functionality exists in health IT presented for certification is the right focus. As with other 2014 Edition functionality, we believe this functionality is fairly ubiquitous now with the widespread adoption of health IT certified to the 2014 Edition. Further, we continue to believe that, for the purposes of certification, having smoking status available for access and exchange via the USCDI is ultimately the key requirement for supporting interoperability.

Removal of Specific USCDI Smoking Status Code Sets

As mentioned above, we believe having smoking status available for USCDI purposes is fundamentally important for supporting interoperability. We propose, however, to remove the requirement to code smoking status according to the adopted eight smoking status SNOMED CT® codes as referenced in the value set in § 170.207(h). These eight codes reflect an attempt to capture smoking status in a consistent manner. Stakeholder feedback has, however, indicated that these eight codes do not appropriately and accurately capture all applicable patients' smoking statuses. Accordingly, we propose to no longer require use of only the specific eight SNOMED CT® codes for representing smoking status (and remove the standard from § 170.207). Rather, to continue to promote interoperability while also granting providers with flexibility to better support clinical care, we propose that health IT would simply be required to be capable of representing smoking status in SNOMED CT® when such information is exchanged as part of the USCDI.

b. Drug-Formulary and Preferred Drug Lists

We propose to remove the 2015 Edition ''drug formulary and preferred drug list checks'' criterion in § 170.315(a)(10). We adopted a 2015 Edition ''drug-formulary and preferred drug list checks'' criterion that separates drug formulary and preferred drug list functionality, but does *not* require any standards or functionality beyond that included in the 2014 Edition ''drug-formulary checks'' criterion. First, we believe this functionality is fairly ubiquitous now with the widespread adoption of health IT certified to the 2014 Edition, which included this general functionality. Second, without standards, this criterion does not support or facilitate the critical goal of health IT interoperability. Therefore, removal of this criterion could reduce health IT developer and health care provider burden.

c. Patient-Specific Education Resources

We propose to remove the 2015 Edition ''patient-specific education resources'' certification criterion (§ 170.315(a)(13)). ONC continues to support patient and provider interaction, and the identification and dissemination of patient-specific educational materials to promote positive health outcomes. However, we no longer believe that certification focused on a health IT's ability to identifying the existence of patient-specific education materials encourages the advancement of this functionality or interoperability. First, this criterion would no longer be associated with an objective or measure under the Promoting Interoperability Programs based on proposals and determinations in recent CMS rulemakings (83 FR 35928; 83 FR 41664). Second, based on the number of health IT products that have been certified for this functionality as part of 2014 Edition certification and already for 2015 Edition certification, we believe that health IT's ability to identify appropriate patient education materials is widespread now among health IT developers and their customers (*e.g.,* health care providers). Third, we have recently seen innovative advancements in this field, including the use of automation and algorithms to provide appropriate educations materials to patients in a timely manner. These advancements help limit clinical workflow interruptions and demonstrate the use and promise of health IT to create efficiencies and improve patient care. As such, removal of this criterion would prevent certification from creating an unnecessary burden for developers and providers and an impediment to innovation.

d. CCDS Summary Record—Create; and CCDS Summary Record—Receive

We assessed the number of products certified to the 2015 Edition ''Common Clinical Data Set summary record—create'' (§ 170.315(b)(4)) and ''Common Clinical Data Set summary record—receive'' (§ 170.315(b)(5)) criteria that have not also been certified to the 2015 Edition ''transitions of care'' criterion (§ 170.315(b)(1)). We did this because the 2015 Edition ''CCDS summary record'' criteria include the same functionality as the 2015 Edition ''transitions of care'' criterion, except for Direct-related transport functionality. Based on our findings of only two unique products certified to these criteria at the time of the drafting of this proposed rule, there appears to be little market demand for certification to them. This outcome is likely attributable to the fact mentioned above regarding their relationship to the 2015 Edition ''transition of care'' criterion, that they are not included in the 2015 Edition Base EHR definition, and that no HHS program specifically requires the use of health IT certified to the criteria. Therefore, we propose to remove these certification criteria from the 2015 Edition.

e. Secure Messaging

We propose to remove the 2015 Edition ''secure messaging'' criterion (§ 170.315(e)(2)). ONC strongly supports patient and provider communication, as well as protecting the privacy and security of patient information. However, we no longer believe that separate certification focused on a health IT's ability to send and receive secure messages between health care providers and patients is necessary. First, this criterion would no longer be associated with an objective or measure under the Promoting Interoperability Programs based on proposals and determinations in recent CMS rulemakings (83 FR 41664; 83 FR 35929). Second, there are multiple other 2015 Edition certification criteria that support patient engagement, such as the 2015 Edition ''view, download, and transmit to 3rd party,'' ''API,'' and ''patient health information capture'' certification criteria. Third, we have seen developers integrate this functionality as part of other patient engagement features, such as patient portals. With these considerations in mind and the lack of a negative impact on health IT interoperability, we believe that the removal of this criterion will help reduce burden and costs, while also spurring further innovations in patient engagement.

5. Removal of Certain ONC Health IT Certification Program Requirements

We propose to remove certain mandatory disclosure requirements and a related attestation requirement under the Program. We believe removal of these requirements will reduce costs and burden for Program stakeholders, particularly health IT developers and ONC–ACBs. We welcome comment on the proposed removal of these requirements and any other certification or Program requirements we should consider for removal.

a. Limitations Disclosures

We propose to remove § 170.523(k)(1)(iii)(B), which requires ONC–ACBs to ensure that certified health IT includes a detailed description of all known material information concerning limitations that a user may encounter in the course of implementing and using the certified health IT, whether to meet ''meaningful use'' objectives and measures or to achieve any other use within the scope of the health IT's certification. We also propose to remove § 170.523(k)(1)(iv)(B) and (C), which state that the types of information required to be disclosed include, but are not limited to: (B) Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified; (C) Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

These disclosure requirements regarding certified health IT limitations are superseded by the Cures Act information blocking provision and Conditions of Certification, which we are implementing with this proposed rule. In particular, section 3001(c)(5)(D)(ii) of the Cures Act requires that a health IT developer, as a Condition of Certification under the Program, provide assurances to the Secretary that, unless for legitimate purposes specified by the Secretary, the developer will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA, or any other action that may inhibit the appropriate exchange, access, and use of electronic health information. These assurances specifically focus on preventing information blocking and promoting appropriate exchange, access, and use of electronic health information. We further propose adding as a complementary Condition of Certification that developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Such actions may inhibit the appropriate access, exchange, or use of electronic health information and are therefore contrary to this proposed Condition of Certification and the statutory provision that it implements. Based on these Conditions of Certification, we believe that disclosures of limitations by health IT developers would be unlikely and unnecessary given their prohibition.

b. Transparency and Mandatory Disclosures Requirements

We propose to remove the Principle of Proper Conduct (PoPC) in § 170.523(k)(2), which requires a health IT developer to submit an attestation that it will disclose all of the information in its mandatory disclosures per § 170.523(k)(1) to specified parties (*e.g.,* potential customers or anyone inquiring about a product quote or description of services). We propose that this provision is no longer necessary and that its removal is appropriate to further reduce administrative burden for health IT developers and ONC–ACBs. First, our experience with developer attestations to this requirement is that over 90% of developers with certified health IT have attested that they will provide ''transparency information.'' Second, the information that developers would be asked to attest to, whether our proposal above to remove certain disclosure requirements is finalized or not, is now readily available on health IT developers' websites as the mandatory disclosure requirements were implemented almost three years ago. Therefore, we believe removal of this requirement is appropriate.

6. Recognition of Food and Drug Administration Processes

Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA), Public Law 112–144, required that the Food and Drug Administration (FDA), in consultation with ONC and the Federal Communications Commission (FCC) (collectively referred to as ''the Agencies'' [10] for this proposal), develop a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health IT, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication. The FDASIA Health IT Report of April 2014 [11] contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health IT that promotes innovation, protects patient safety, and avoids regulatory duplication. Public comments, received prior to the report and after,[12] recommended that health IT developers/manufacturers apply a single process that satisfies the requirements of all agencies and that existing safety and quality-related processes, systems, and standards should be leveraged for patient safety in health IT. On July 27, 2017, FDA announced a voluntary Software Precertification (Pre-Cert) Pilot Program as part of a broader Digital Health Innovation Action Plan.[13] It was developed in order to create a tailored approach toward recognizing the unique characteristics of digital technology by looking first at the firm, rather than primarily at each product of the firm, as is currently done for traditional medical products. The FDA plans to explore whether and how pre-certified companies that have demonstrated a culture of quality, patient safety, and organizational excellence could bring certain types of digital health products to market either without FDA premarket review or with a more streamlined FDA premarket review.

a. FDA Software Pre-Certification Pilot Program

ONC believes that health IT developers that hold precertification under the FDA Digital Health Software Precertification Program (FDA Software Precertification Program) when they present health IT for certification under the Program could qualify for, and benefit from, further efficiencies under the Program. Title IV of the Cures Act provides ONC with authority under the Program to oversee health IT developers through Conditions and Maintenance of Certification requirements (*see* section VII Conditions and Maintenance of Certification of this proposed rule). With this new authority and our authority over health IT developers' health IT certified under the Program, we propose to establish processes that would provide health IT developers that can document holding precertification under the FDA Software Precertification Program with exemptions to the ONC Health IT Certification Program's requirements for testing and certification of its health IT to the 2015

[10] ONC is not an agency, but an Office, within the Department of Health and Human Services.

[11] *https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf.*

[12] *https://www.federalregister.gov/documents/2013/05/30/2013-12817/food-and-drug-administration-safety-and-innovation-act-fdasia-request-for-comments-on-the; https://blogs.fda.gov/fdavoice/index.php/2014/04/fda-seeks-comment-on-proposed-health-it-strategy-that-aims-to-promote-innovation/;* and *https://www.regulations.gov/document?D=FDA-2014-N-0339-0001.*

[13] *https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/Default.htm.*

Edition ‘‘quality management systems’’ criterion (§ 170.315(g)(4)) and the 2015 Edition ‘‘safety-enhanced design’’ criterion (§ 170.315(g)(3)), as these criteria are applicable to the health IT developer's health IT presented for certification. We also believe that such a ‘‘recognition’’ could, depending on the final framework of the FDA Software Precertification Program (*e.g.,* the key performance indicators used to demonstrate performance and outcomes of excellence), be applicable to the functionally-based 2015 Edition ‘‘clinical’’ certification criteria (§ 170.315(a)). More specifically, this could address the ‘‘computerized provider order entry (CPOE)’’ (§ 170.315(a)(1), (2), and (3)), ‘‘drug-drug, drug-allergy interaction checks for CPOE’’ (§ 170.315(a)(4)), ‘‘clinical decision support’’ (§ 170.315(a)(9)), and ‘‘implantable device list’’ (§ 170.315(a)(14)) certification criteria. Such ‘‘recognition’’ could also be appropriate to address any or all of the following functionally-based 2015 Edition criteria in the event their proposed removal is not finalized: ‘‘problem list’’ (§ 170.315(a)(6)), ‘‘medication list’’ (§ 170.315(a)(7)), ‘‘medication allergy list’’ (§ 170.315(a)(8)), ‘‘drug-formulary and preferred drug list checks’’ (§ 170.315(a)(10)),’’ and ‘‘smoking status’’ (§ 170.315(a)(11)).

Our proposed ‘‘recognition’’ would align with both Executive Orders 13563 and 13771 regarding deregulatory, less burdensome, and more effective initiatives. It would also serve as a regulatory relief for those health IT developers qualifying as small businesses under the Regulatory Flexibility Act (*see* section XIV.C.3 Regulatory Flexibility Act of this proposed rule). Furthermore, it would closely align with FDASIA's instruction to promote innovation, protect patient safety, and avoid regulatory duplication. However, despite these proffered benefits, there may be reasons not to adopt such a ‘‘recognition’’ approach. For example, stakeholders may not agree that the FDA Software Precertification Program (and/or subsequent finalized program) sufficiently aligns with our Program. Developers and providers may have varying and divergent views about the benefits and detriments of such an approach. Further, while we believe that we could properly operationalize such an approach by ensuring certifications indicate which criteria have been ‘‘deemed certified’’ by ONC (but still subject to ONC–ACB surveillance), stakeholders may have other operational concerns. Accordingly, we welcome comments on these and other aspects of our proposed ‘‘recognition’’ approach, including the 2015 Edition certification criteria that should be eligible for ‘‘recognition.’’

b. Development of Similar Independent Program Processes—Request for Information

Recognition of the FDA Software Pre-Certification Program for purposes of our Program, as noted above, may eventually be determined to be infeasible or insufficient to meet our goals of reducing burden and promoting innovation. With this in mind, we request comment on whether ONC should establish new regulatory processes tailored towards recognizing the unique characteristics of health IT (*e.g.,* EHR software) by looking first at the health IT developer, rather than primarily at the health IT presented for certification, as is currently done under the Program. For example, ONC could possibly establish Conditions and Maintenance of Certification requirements, through rulemaking, that facilitate the deeming of all of a health IT developer's health IT as ‘‘certified’’ under the Program for certification criteria identified by ONC as solely ‘‘functionally-based’’ criteria (*i.e.,* not essential to interoperability, such as the ‘‘CPOE’’ criteria) or possibly broader in scope. This approach could rely on, but not be limited to, one or a combination of the following: (1) Certain demonstrated health IT developer processes or health IT functionality; (2) prior successful certification of a health IT developer's health IT under the Program; (3) results of real world testing for interoperability as required by the Cures Act and the proposed implementing regulatory Condition of Certification (*see* section VII.B.5 of this proposed rule); and/or (4) the results of the EHR Reporting Program once implemented (*see* section VII.B.7 of this proposed rule). No matter the specifics, we are most interested in whether stakeholders believe this is an approach we should pursue in conjunction with, or in lieu of, the proposed approach of recognizing the FDA Software Pre-Certification Pilot Program. We also welcome more specific comments on the health IT developer criteria for such an approach and what the Conditions and/or Maintenance of Certification requirements should be to support such an approach within the framework of the proposed Conditions and Maintenance of Certification requirements discussed in section VII of this proposed rule.

IV. Updates to the 2015 Edition Certification Criteria

This rule proposes to update the 2015 Edition by revising and adding certification criteria that would establish the capabilities and related standards and implementation specifications for the certification of health IT. The updates to the 2015 Edition would enhance interoperability and improve the accessibility of patient records consistent with section 4006(a) of the Cures Act.

A. Standards and Implementation Specifications

1. National Technology Transfer and Advancement Act

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 [14] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to electing only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. Agencies have the discretion to decline the use of existing voluntary consensus standards if determined that such standards are inconsistent with applicable law or otherwise impractical, and instead use a government-unique standard or other standard. In addition to the consideration of voluntary consensus standards, the OMB Circular A–119 recognizes the contributions of standardization activities that take place outside of the voluntary consensus standards process. Therefore, in instances where use of voluntary consensus standards would be inconsistent with applicable law or otherwise impracticable, other standards should be considered that meet the agency's regulatory, procurement or program needs, deliver favorable technical and economic outcomes, and are widely utilized in the marketplace. In this proposed rule, we use voluntary consensus standards except for:

- The standard we propose to adopt in § 170.213. We propose to remove the Common Clinical Data Set (CCDS) definition and effectively replace it with a government

[14] *https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A119/revised_circular_a-119_as_of_1_22.pdf.*

unique standard, the United States Core Data for Interoperability (USCDI), Version 1(v1);

- The standard we propose to adopt in § 170.215(a)(2). We propose the government unique API Resource Collection in Health (ARCH) Version 1 implementation specification;
- The standards we propose to adopt in § 170.215(a)(3) through (5) for application programming interfaces (APIs). These market driven consortia standards have been developed through a streamlined process that does not meet the full definition of voluntary consensus standards development but still includes representation from those interested in the use cases supported by the standards (*e.g.,* health IT developers and health care providers). In the absence of available voluntary consensus standards that would meet our needs, these standards deliver favorable technical and economic outcomes, particularly improved interoperability. Further, some of these standards may eventually proceed through a standards development organization for approval; and
- The standards we propose to adopt in § 170.205(h)(3) and (k)(3). We propose to replace the current HL7 QRDA standards with government unique standards that more effectively support the associated certification criterion's use case, which is reporting eCQM data to CMS.

2. Compliance With Adopted Standards and Implementation Specifications

In accordance with Office of the Federal Register regulations related to ''incorporation by reference,'' 1 CFR part 51, which we follow when we adopt proposed standards and/or implementation specifications in any subsequent final rule, the entire standard or implementation specification document is deemed published in the **Federal Register** when incorporated by reference therein with the approval of the Director of the Federal Register. Once published, compliance with the standard and implementation specification includes the entire document unless we specify otherwise. For example, if we adopted the Argonaut Data Query Implementation Guide (IG) proposed in this proposed rule (*see* section VII.B.4.b), health IT certified to certification criteria referencing this IG would need to demonstrate compliance with all mandatory elements and requirements of the IG. If an element of the IG is optional or permissive in any way, it would remain that way for testing and certification *unless* we specified otherwise in regulation. In such cases, the regulatory text would preempt the permissiveness of the IG.

3. ''Reasonably Available'' to Interested Parties

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies propose to incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(a)). To comply with these requirements, in section XI (''Incorporation by Reference'') of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we propose to adopt and subsequently incorporate by reference in the Code of Federal Regulations. To note, we also provide relevant information about these standards and implementation specifications throughout the relevant sections of the proposed rule.

B. Revised and New 2015 Edition Criteria

In order to capture and share patient data efficiently, health care providers need health IT that store data in structured formats. Structured data allows health care providers to easily retrieve and transfer patient information, and use health IT in ways that can aid patient care. We propose to adopt revised and new 2015 Edition certification criteria, including new standards, to support these objectives. Some of these criteria and standards are included in the Certified EHR Technology (CEHRT) definition used for participation in HHS Programs, such as the Promoting Interoperability Programs (formerly the EHR Incentive Programs), some are required to be met for participation in the ONC Health IT Certification Program, and some, though beneficial, are unassociated with the CEHRT definition and not required for participating in any HHS program, including the ONC Health IT Certification Program.

1. The United States Core Data for Interoperability Standard (USCDI)

The initial focus of the Program was to support the Medicare and Medicaid EHR Incentive Programs (76 FR 1294) now referred to as the Promoting Interoperability Programs (and referenced as such hereafter). As such, the 2014 Edition certification criteria mirrored those functions specified by Promoting Interoperability Programs' objectives and measures. In order to improve efficiency and streamline the common data within our Program's certification criteria, we created a single definition for all the required data which could be referenced for all applicable certification criteria. We created the term ''Common MU Data Set'' to encompass the common set of MU data types/elements (and associated vocabulary standards) for which certification would be required across several certification criteria (77 FR 54170).

The 2015 Edition final rule modified the Program to make it open and accessible to more types of health IT, and health IT that supports various care and practice settings beyond those included in the Promoting Interoperability Programs (80 FR 62604). In comparison to the previous editions, the 2015 Edition focused on identifying health IT components necessary to establish an interoperable nationwide health information infrastructure, fostering innovation and open new market opportunities, and allowing for more health care provider and patient choices in electronic health information access and exchange. In order to align with this approach, we revised the concept of the ''Common MU Data Set'' definition and changed the name to the ''Common Clinical Data Set'' (CCDS) definition. The CCDS definition was further revised in the 2015 Edition rulemaking to account for new and updated vocabulary and content standards in order to improve and advance interoperability and health information exchange (80 FR 62604). It further expanded accessibility and availability of data exchanged by updating the definition of Base Electronic Health Record (EHR) (2015 Edition Base EHR definition) to include enhanced data export, transitions of care, and application programming interface (API) capabilities, all of which required that at a minimum the CCDS be available (80 FR 62602–62604).

The regulatory approach to use and reference a ''definition'' to identify electronic health information, including with associated vocabulary codes, for access, exchange and use has had its drawbacks. While the CCDS definition served its designed purpose, to cut down on repetitive text in each of the certification criteria in which it is referenced, it also began to be colloquially used for many different purposes. As the CCDS definition's relevance grew outside of its regulatory context it became a symbolic and practical limit to the industry's collective interests to go beyond the CCDS data for access, exchange, and use. As we move towards value-based care and the inclusion of data classes that go beyond clinical data, and as part of ONC's continued efforts to evaluate the availability of a minimum baseline of data classes that must be commonly available for interoperable exchange, we acknowledge the need to change and improve our regulatory approach to the CCDS. Therefore, in order to advance interoperability by ensuring compliance with new data and vocabulary codes sets that support the data, we propose to remove the ''Common Clinical Data Set'' definition and its references from the 2015 Edition and replace it with the ''United States Core Data for Interoperability'' (USCDI) standard. The USCDI standard aims to achieve the goals set forth in the Cures Act by specifying a common set of data classes for interoperable exchange.

We propose to adopt the USCDI as a standard as such term is defined in § 170.102. In § 170.102, a ''standard'' is defined as a ''technical, functional, or performance-based rule, condition, requirement, or specification that stipulates instructions, fields, codes, data, materials, characteristics, or actions.'' The USCDI standard would comprise data classes, which may be further delineated into groupings of specific data element(s). For example, ''patient demographics'' is a data class and within that data class there is ''patient name,'' which is a data element. As noted in section IV.B.1.b, for the overall structure and organization of the USCDI, please consult *www.healthIT.gov/USCDI.*

ONC intends to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. Once the Secretary adopts the first version of the USCDI through rulemaking, which we propose in this rulemaking, health IT developers would be allowed to take advantage of the ''Standards Version Advancement Process'' flexibility. The Standards Version Advancement Process, proposed in Section VII.B.5 (below), would permit health IT developers to voluntarily implement and use a new version of an adopted standard (*e.g.,* the USCDI), subject to certain conditions including a requirement that the new version is approved for use by the National Coordinator.

a. USCDI 2015 Edition Certification Criteria

We propose to adopt the USCDI Version 1 (USCDI v1) in § 170.213. [15] The USCDI is a standardized set of health data classes and constituent data elements that would be required to support nationwide electronic health information exchange. Once adopted in a final rule, health IT developers would be required to update their certified health IT to support the USCDI v1 for all certification criteria affected by this proposed change. We propose to revise the following CCDS dependent 2015 Edition certification criteria to incorporate the USCDI standard:

- ''Transitions of care'' (§ 170.315(b)(1));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6));
- ''transmission to public health agencies—electronic case reporting'' (§ 170.315(f)(5)); and
- ''application access—all data request'' (§ 170.315(g)(9)).

We note that we did not include the ''data export'' criterion (§ 170.315(b)(6)) as we are proposing to remove it and adopt instead the ''EHI export'' criterion (§ 170.315(b)(10)). For similar reasons, we did not include the ''application access—data category request'' criterion (§ 170.315(g)(8)) because we are proposing to replace it with the API certification criterion (§ 170.315(g)(10)), which derives its data requirements from the USCDI.

We propose, as a Maintenance of Certification requirement for the real world testing Condition of Certification, that health IT developers with health IT certified to the five above-identified certification criteria prior to the effective date of a subsequent final rule would have to update such certified health IT to the proposed revisions. We further propose, as a Maintenance of Certification requirement for the real world testing Condition of Certification, that health IT developers must provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the effective date of a final rule for this proposed rule. For the purposes of meeting this compliance timeline, we expect health IT developers to update their certified health IT without new mandatory testing and notify their ONC–ACB on the date at which they have reached compliance. Developers would also need to factor these updates into their next real world testing plan as discussed in section VII.B.5 of this proposed rule. Further, we refer health IT developer to the next section, which describes how the USCDI differs from the current CCDS.

b. USCDI Standard—Data Classes Included

The USCDI Version 1 (USCDI v1) and its constituent data elements account for the public comments we received on the Draft USCDI and Proposed Expansion Process[16] published in January 2018 as well as initial feedback from the Health IT Advisory Committee. The standard as we propose to adopt it in § 170.213 also reflects and acknowledges the burden that rapidly expanding the USCDI v1 beyond the CCDS could cause. As a result, the USCDI v1 is a modest expansion of the CCDS, which we believe most health IT developers already support, were already working toward, or should be capable of updating their health IT to support in a timely manner. The following describes only the delta between the CCDS and the USCDI v1. For the overall structure and organization of the USCDI standard, please consult *www.healthIT.gov/USCDI.*

i. Updated Versions of Vocabulary Standard Code Sets

We propose that the USCDI Version 1 (USCDI v1) include the newest versions of the ''minimum standard'' code sets included in the CCDS available at publication of a subsequent final rule. We request comment on this proposal and on whether this could result in any interoperability concerns. To note, criteria such as the 2015 Edition ''family health history'' criterion (§ 170.315(a)(12)), the 2015 Edition ''transmission to immunization registries'' criterion (§ 170.315(f)(1)), and the 2015 Edition ''transmission to public health agencies—syndromic surveillance'' criterion (§ 170.315(f)(2)) reference ''minimum standard'' code sets; however, we are considering changing the certification baseline versions of the code set for these criteria from the versions adopted in the 2015 Edition final rule to ensure complete interoperability alignment. We welcome comment on whether we should adopt such an approach.

We also note, for purposes of clarity, that consistent with § 170.555, unless the Secretary prohibits the use of a newer version of an identified minimum standard code set for certification, health IT could continue to be certified or upgraded to a newer version of an identified minimum standard code set than that included in USCDI v1 or the most recent USCDI version that the National Coordinator has approved for use in the Program via the Standards Version Advancement Process.

ii. Address and Phone Number

The USCDI v1 includes new data elements for ''address'' and ''phone number.'' The inclusion of ''address'' (to represent the postal location for the

[15] We note that USCDI v1is an updated version and distinguished from the *Draft United States Core Data for Interoperability (USCDI)* previously made available for public review and comment in the course of its development as a prospective standard.

[16] *https://www.healthit.gov/sites/default/files/draft-uscdi.pdf.*

patient) and ''phone number'' (to represent the patient's telephone number) would improve the comprehensiveness of health information for patient care. The inclusion of these data elements is also consistent with the list of patient matching data elements already specified in the 2015 Edition ''transitions of care'' certification criterion (§ 170.315(b)(1)(iii)(G)), which supports the exchange of patient health information between providers of patient care.

iii. Pediatric Vital Signs

The USCDI v1 includes the pediatric vital sign data elements, which are specified as optional health information in the 2015 Edition CCDS definition. Pediatric vital signs include: Head occipital-frontal circumference for children less than 3 years of age, BMI percentile per age and sex for youth 2–20 years of age, weight for age per length and sex for children less than 3 years of age, and the reference range/scale or growth curve, as appropriate. As explained in section VI.A.2 of this proposed rule, the inclusion of pediatric vital sign data elements in the draft USCDI v1 would align with the provisions of the Cures Act related to health IT to support the health care of children. Stakeholders emphasized the value of pediatric vital sign data elements to better support the safety and quality of care delivered to children. We also note that, as discussed in the 2015 Edition proposed rule, the Centers for Disease Control and Prevention (CDC) recommends the use of these pediatric vital signs for settings of care in which pediatric and adolescent patients are seen (80 FR 16818–16819) as part of best practices. The availability of a reference range/scale or growth curve would help with proper interpretation of the measurements for the BMI percentile per age and sex and weight for age per length and sex. Further, the inclusion of this health information in the USCDI v1 is the appropriate next step after first specifying them as optional in the CCDS definition as part of the 2015 Edition rulemaking and as a means of supporting patient access to their EHI in a longitudinal format through certified health IT (*see* section 3009(e)(2)(A)(i) of the PHSA as amended by the Cures Act). We recognize, however, that certain health IT developers and their customers may not find these capabilities and information useful. Therefore, we request comment on the inclusion of pediatric vital signs in the USCDI v1, including the potential benefits and costs for all stakeholders stemming from its inclusion in the USCDI v1.

iv. Clinical Notes

The USCDI v1 includes a new data class, titled ''clinical notes.'' ''Clinical notes'' is included in the USCDI v1 based on significant feedback from the industry since the 2015 Edition final rule. We also received feedback during the Trusted Exchange Framework and Common Agreement (TEFCA) stakeholder sessions and public comment period. It has been identified by stakeholders as highly desirable data for interoperable exchange. The free text portion of the clinical notes was most often relayed by clinicians as the data they sought, but were often missing during electronic health information exchange. Clinical notes can be composed of text generated from structured (pick-list and/or check the box) fields as well as unstructured (free text) data. A clinical note may include the assessment, diagnosis, plan of care and evaluation of plan, patient teaching, and other relevant data points.

We recognize that a number of different clinical notes could be useful for stakeholders. It is our understanding that work is being done in the community to focus on a subset of clinical notes. We considered three options for identifying the different ''note types'' to adopt in USCDI v1. The first option we considered would allow for the community to offer any and all recommended notes. The second option we considered would set a minimum standard of eight note types. This option was derived from the eight note types identified by the Argonaut Project participants.[17] The third option we identified would look to the eleven HL7 Consolidated Clinical Data Architecture (C–CDA) document types identified in the C–CDA Release 2.1, which also included the note types being identified by the Argonaut Project participants. We ultimately decided to move forward with the second option because it unites public and private interests toward the same goal. The eight selected note types are a minimum bar and, in the future, the USCDI may be updated to include other clinical notes. Specifically, we propose to include the following clinical note types for both inpatient and outpatient (primary care, emergency department, etc.) settings in USCDI v1 as a minimum standard: (1) Discharge Summary note; (2) History & Physical; (3) Progress Note; (4) Consultation Note; (5) Imaging Narrative; (6) Laboratory Report Narrative; (7) Pathology Report Narrative; and (8) Procedures Note. We seek comment on whether to include additional note types as part of the USCDI v1.

v. Provenance

The USCDI v1 also includes a new data class, titled ''provenance.'' ''Provenance'' has been identified by stakeholders[18] as valuable for interoperable exchange. The provenance of data was also referenced by stakeholders as a fundamental need to improve the trustworthiness and reliability of the data being exchanged. Provenance describes the metadata, or extra information about data, that can help answer questions such as when and who created the data.

The inclusion of ''provenance'' as a data class in the USCDI v1 would also complement the Cures Act requirement to support the exchange of data through the use of APIs. This approach differs from the exchange of data via the C–CDA. While C–CDAs are often critiqued due to their relative ''length,'' the C–CDA represents the output of a clinical encounter and includes relevant context. The same will not always be true in an API context. APIs facilitate the granular exchange of data and, as noted in the 2015 Edition final rule, offer the potential to aggregate data from multiple sources in a web or mobile application (80 FR 62675). The inclusion of provenance would help retain the relevant context so the recipient can better understand the origin of the data. As noted in section VII.B.4, we are also proposing to include provenance in our proposed ''API Resource Collection in Health'' (ARCH) Version 1 implementation specification in § 170.215(a)(2), which would list a set of base Fast Healthcare Interoperability Resources (FHIR®) resources that Health IT Modules certified to the proposed API criterion (§ 170.315(g)(10)) would need to support.

We propose to further delineate the provenance data class into three data elements: ''the author,'' which represents the person(s) who is responsible for the information; ''the author's time stamp,'' which indicates the time the information was recorded; and ''the author's organization,'' which would be the organization the author is associated with at the time they interacted with the data. We have identified these three data elements as fundamental for data recipients to have

[17] Link to the Clinical Notes Argonaut Project identified (to clarify: Seven bullets are listed, however, we split laboratory and pathology note types into their own note) *http://wiki.hl7.org/index.php?title=201805_Clinical_Notes_Track.*

[18] *https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement.*

available and both are commonly captured and currently available through standards. We request comment on the inclusion of these three data elements and whether any other provenance data elements, such as the identity of the individual or entity the data was obtained from or sent by (sometimes discussed in standards working groups as the provenance of the data's ''last hop''), would be essential to include as part of the USCDI v1 standard. We acknowledge that there is currently work to help define provenance in a standard robust manner, and we anticipate adopting the industry consensus once it becomes available.

vi. Unique Device Identifier(s) for a Patient's Implantable Device(s)

We are aware of a recently published implementation guide (IG) within HL7 that provides further guidance on the unique device identifier (UDI) requirements. The IG, Health Level 7 (HL7®) CDA R2 Implementation Guide: C–CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1–US Realm,[19] identifies changes needed to the C–CDA to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. The UDI components include the Device Identifier (DI) and the following individual production identifiers: The lot or batch number, serial number, manufacturing date, expiration date, and distinct identification code. However, as this new IG has been recently published, we request comment on whether we should add this UDI IG as a requirement for health IT to adopt in order to meet the requirements for UDI USCDI Data Class. In addition, we do not have a reliable basis on which to estimate how much it would cost to meet the requirements outlined in the UDI IG; and, therefore, we request comment on the cost and burden of complying with this proposed requirement.

vii. Medication Data Request for Comment

The USCDI v1 ''Medication'' data class includes two constituent data elements within it: Medications and Medication Allergies. With respect to the latter, Medication Allergies, we request comment on an alternative approach. This alternative would result in removing the Medication Allergies data element from the Medication data class and creating a new data class titled, ''Substance Reactions,'' which would be meant to be inclusive of ''Medication Allergies.'' The new ''Substance Reactions'' data class would include the following data elements: ''Substance'' and ''Reaction,'' and include SNOMED CT as an additional applicable standard for non-medication substances.

c. USCDI Standard—Relationship to Content Exchange Standards and Implementation Specifications

In order to align with our approach to be responsive to the evolution of standards and to facilitate updates to newer versions of standards, the USCDI v1 (§ 170.213) is ''content exchange'' standard agnostic. It establishes ''data policy'' and does not directly associate with the content exchange standards and implementation specifications which, given a particular context, may be necessary to exchange the entire USCDI, a USCDI class, or elements within it. To our knowledge, all data classes in the USCDI v1 can be supported by commonly used ''content exchange'' standards, including HL7 C–CDA Release 2.1 and FHIR®.

d. Clinical Notes C–CDA Implementation Specification

In conjunction with our proposal to adopt the USCDI v1, we propose to adopt the HL7 CDA® R2 IG: C–CDA Templates for Clinical Notes R1 Companion Guide, Release 1 in § 170.205(a)(4)(i) (''C–CDA Companion Guide''). The C–CDA Companion Guide provides supplemental guidance and additional technical clarification for specifying data in the C–CDA Release 2.1.[20] As noted above, the proposed USCDI v1 includes new data classes, such as ''clinical notes,'' which are further supported through the C–CDA Companion Guide. For example, the C–CDA Companion Guide provides specifications for clinical notes by indicating that clinical notes should be recorded in ''note activity'' and requires references to other discrete data, such as ''encounters.'' The C–CDA Companion Guide also enhances implementation of the 2015 Edition certification criteria that reference the C–CDA Release 2.1 (§ 170.205(a)(4)). As noted by stakeholders, the C–CDA Release 2.1 includes some optionality and ambiguity with respect to data element components, such as the locations and value sets. We attempted to address some of this optionality by clarifying requirements using Certification Companion Guides (CCGs)[21] and by specifying in the CCDS definition where certain data should be placed in the C–CDA Release 2.1 templates (*e.g.,* ''goals'' in the goals section).[22] The C–CDA Companion Guide, which was released after the 2015 Edition final rule, provides similar, but additional C–CDA implementation structure. For example, race and ethnicity are required data elements in the USCDI (formerly the CCDS) and must be included in C–CDA exchanges if known, or they may be marked with a nullFlavor of UNK (unknown) if not known. The C–CDA Release 2.1 is unclear on the location and value set, but the C–CDA Companion Guide clarifies the location and value set. The adoption of the C–CDA Companion Guide would align with our goal to increase the consistent implementation of standards among health IT developers and improve interoperability. We propose to adopt this C–CDA Companion Guide to support best practice implementation of USCDI v1 data classes and 2015 Edition certification criteria that reference C–CDA Release 2.1 (§ 170.205(a)(4)). The criteria include:

- ''Transitions of care'' (§ 170.315(b)(1));
- ''clinical information reconciliation and incorporation'' (§ 170.315(b)(2));
- ''care plan'' (§ 170.315(b)(9));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6)); and
- ''application access—all data request'' (§ 170.315(g)(9)).

We propose, as a Maintenance of Certification requirement for the real world testing Condition of Certification, that health IT developers with health IT certified to the six above-identified certification criteria prior to the effective date of a subsequent final rule would have to update such certified health IT to the proposed revisions. We further propose, as a Maintenance of Certification requirement for the real world testing Condition of Certification, that health IT developers must provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the effective date of a final rule for this proposed rule. For the purposes of meeting this compliance timeline, we expect health IT developers to update their certified health IT without new mandatory testing and notify their

[19] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=486.*

[20] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=447.*

[21] *https://www.healthit.gov/topic/certification-ehrs/2015-edition-test-method.*

[22] *https://www.healthit.gov/sites/default/files/topiclanding/2018-04/2015Ed_CCG_CCDS.pdf.*

ONC–ACB on the date at which they have reached compliance. Developers would also need to factor these updates into their next real world testing plan as discussed in section VII.B.5 of this proposed rule.

2. Electronic Prescribing Standard and Certification Criterion

We propose to update the electronic prescribing (e-Rx) SCRIPT standard used for ‘‘electronic prescribing’’ in the 2015 Edition to NCPDP SCRIPT 2017071, which would result in a new e-Rx standard becoming the baseline for certification. We propose to adopt this standard in § 170.205(b)(1). ONC and CMS have historically maintained complementary policies of aligning health IT certification criteria and associated standard for e-prescribing with the CMS Medicare Part D e-Rx and MH standards (75 FR 44589; 77 FR 54198). To this end, CMS has retired the current standard (NCPDP SCRIPT version 10.6) for e-RX and MH and adopted NCPDP SCRIPT 2017071 as the standard for Part D e-Rx and MH effective January 1, 2020, conditional on ONC updating the Program to the NCPDP SCRIPT 2017071 standard for its e-Rx certification criterion (*see also* 42 CFR 423.160(b)(1)(v) and (2)(iv)). In addition, CMS recently sought comment regarding whether the NCPDP SCRIPT 2017071 standard could facilitate future reporting of the proposed Query of Prescription Drug Monitoring Program (PDMP) measure in both the 2019 Physician Fee Schedule proposed rule (83 FR 35923) and Hospital Inpatient Prospective Payment Systems (IPPS) Fiscal Year 2019 proposed rule (83 FR 20528).

As summarized in the IPPS Fiscal Year 2019 final rule (83 FR 41144), CMS received comments supportive of using the NCPDP SCRIPT 2017071 medication history transactions for PDMP queries and responses, as well as comments asking CMS to seek harmonizing of the 2015 Edition e-prescribing certification criterion to the NCPDP SCRIPT 2017071 standard specified in the part D program portions of the recent ‘‘Medicare Program; Contract Year 2019 Policy and Technical Changes to the Medicare Advantage, Medicare Cost Plan, Medicare Fee-for-Service, the Medicare Prescription Drug Benefit Programs, and the PACE Program’’ final rule (83 FR 16440).

In addition to proposing to adopt the NCPDP SCRIPT 2017071 standard for the transactions that are listed in the current ‘‘electronic prescribing’’ criterion (§ 170.315(b)(3)), we propose to adopt and require conformance to all of the NCPDP SCRIPT 2017071 standard transactions CMS adopted at 42 CFR 423.160(b)(2)(iv) for NCPDP SCRIPT 2017071. Therefore, we propose to adopt a new 2015 Edition ‘‘electronic prescribing’’ criterion (§ 170.315(b)(11)) that includes the following transactions:

- Create new prescriptions (NewRx, NewRxRequest, NewRxResponseDenied)

A NewRx transaction is a new prescription from a prescriber to a pharmacy so that it can be dispensed to a patient. A NewRxRequest is a request from a pharmacy to a prescriber for a new prescription for a patient. A NewRxResponseDenied is a denied response to a previously sent NewRxRequest (if approved, a NewRx would be sent). A NewRxResponseDenied response may occur when the NewRxRequest cannot be processed or if information is unavailable.

- Change prescriptions (RxChangeRequest, RxChangeResponse)

An RxChangeRequest transaction originates from a pharmacy to request: A change in the original prescription (new or fillable), validation of prescriber credentials, a prescriber to review the drug requested, or a prior authorization from the payer for the prescription. An RxChangeResponse transaction originates from a prescriber to respond: To a prescription change request from a pharmacy, to a request for a prior authorization from a pharmacy, or to a prescriber credential validation request from a pharmacy.

- Cancel prescriptions (CancelRx, CancelRxResponse)

A CancelRx transaction is a request from a prescriber to a pharmacy to not fill a previously sent prescription. A CancelRx must contain pertinent information for the pharmacy to be able to find the prescription in their system (patient, medication (name, strength, dosage, form), prescriber, prescription number if available). A CancelRxResponse is a response from a pharmacy to a prescriber to acknowledge a CancelRx, and is used to denote if the cancellation is Approved or Denied.

- Renew prescriptions (RxRenewalRequest, RxRenewalResponse)

An RxRenewalRequest transaction originates from a pharmacy to request additional refills beyond those originally prescribed. RxRenewalResponse originates from a prescriber to respond to the request.

- Receive fill status notifications (RxFill, RxFillIndicatorChange)

An RxFill transaction is sent from a pharmacy to a prescriber or a long term or post-acute care (LTPAC) facility indicating the FillStatus (dispensed, partially dispensed, not dispensed or returned to stock, transferred to another pharmacy) of the new, refill, or resupply prescriptions for a patient. RxFillIndicator informs the pharmacy of the prescriber's intent for fill status notifications for a specific patient/medication. An RxFillIndicatorChange is sent by a prescriber to a pharmacy to indicate that the prescriber is changing the types of RxFill transactions that were previously requested, where the prescriber may modify the fill status of transactions previously selected or cancel future RxFill transactions.

- Request and receive medication history (RxHistoryRequest, RxHistoryResponse)

An RxHistoryRequest transaction is a request from a prescriber for a list of medications that have been prescribed, dispensed, claimed, or indicated by a patient. This request could be sent to a state Prescription Drug Monitoring Program (PDMP). An RxHistoryResponse is a response to an RxHistoryRequest containing a patient's medication history. It includes the medications that were dispensed or obtained within a certain timeframe, and optionally includes the prescriber that prescribed it. RxHistoryRequest and RxHistoryResponse transactions may be sent directly or through an intermediary.

- Ask the Mailbox if there are any transactions (GetMessage)

This transaction is used by the prescriber or pharmacy asking the mailbox if there are any transactions. It is at the heart of the mechanism used by a pharmacy or prescriber system to receive transactions from each other or from a payer or the REMS Administrator via a Switch, acting as a Mailbox.

- Relay acceptance of a transaction back to the sender (Status)

This transaction is used to relay acceptance of a transaction back to the sender. A Status in response to any applicable transaction other than GetMessage indicates acceptance and responsibility for a request. A Status in response to GetMessage indicates that no mail is waiting for pickup. A Status cannot be mailboxed and may not contain an error.

- Respond that there was a problem with the transaction (Error)

This transaction indicates an error has occurred, indicating the request was terminated. An Error can be generated when there is a communication problem or when the transaction actually had an error. An error can be mailboxed, as it may be signifying to the originator that a transaction was unable to be delivered or encountered problems in the acceptance. The Error must be a different response than a Status, since the communication between the system and the Mailbox must clearly denote the actions taking place. An Error is a response being delivered on behalf of a previous transaction, and the Status signifies no more mail.

- Respond that a transaction requesting a return receipt has been received (Verify)

This transaction is a response to a pharmacy or prescriber indicating that a transaction requesting a return receipt has been received. Verifications results when a ''return receipt requested'' flag is set in the original request. Upon receiving a transaction with ReturnReceipt set, it is the responsibility of the receiver to either generate a Verify in response to the request (recommended) or generate a Status in response to this request, followed subsequently by a free standing Verify. This transaction notifies the originator that the transaction was received at the software system. It is not a notification of action taking place, since time may elapse before the ultimate answer to the transaction may take place.

- Request to send an additional supply of medication (Resupply)

This transaction is a request from a Long Term or Post-Acute Care (LTPAC) organization to a pharmacy to send an additional supply of medication for an existing order. An example use case is when a medication supply for a resident is running low (2–3 doses) and a new supply is needed from the pharmacy, the LTPAC organization need a way to notify the pharmacy that an additional supply for the medication is needed.

- Communicate drug administration events (DrugAdministration)

This transaction communicates drug administration events from a prescriber/care facility to the pharmacy or other entity. It is a notification from a prescriber/care facility to a pharmacy or other entity that a drug administration event has occurred—for example, a medication was suspended or administration was resumed.

- Transfer one or more prescriptions (RxTransferRequest, RxTransferResponse, RxTransferConfirm)

The RxTransferRequest transaction is used when the pharmacy is asking for a transfer of one or more prescriptions for a specific patient to the requesting pharmacy. The RxTransferResponse transaction is the response to the RxTransferRequest which includes the prescription(s) being transferred or a rejection of the transfer request. It is sent from the transferring pharmacy to the requesting pharmacy. The RxTransferConfirm transaction is used by the pharmacy receiving (originally requesting) the transfer to confirm that the transfer prescription has been received and the transfer is complete.

- Recertify the continued administration of a medication order (Recertification)

This transaction is a notification from a facility, on behalf of a prescriber, to a pharmacy recertifying the continued administration of a medication order. An example use is when an existing medication order has been recertified by the prescriber for continued use. Long term or post-acute care use only.

- Complete Risk Evaluation and Mitigation Strategy (REMS) Transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse)

With CMS' recent adoption of these transactions in their recently issued final rule associated with e-prescribing for Medicare Part D (42 CFR 423.160(b)(2)(iv)(W)–(Z)), we believe that it would be equally beneficial to include these four REMS transactions as part of this proposed certification criterion: REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse.

The Food and Drug Administration Amendments Act (FDAAA) of 2007 (Pub. L. 110–85) enables the Food and Drug Administration (FDA) to require a REMS from a pharmaceutical manufacturer if the FDA determines that a REMS is necessary to ensure the benefits of a drug outweigh the risks associated with the drug. The currently approved REMS programs vary in levels of complexity. Typically a Med Guide and Communication Plan is required, but some also require Elements to Assure Safe Use (ETASU). The large majority of existing REMS programs are for drugs dispensed through specialty pharmacies, clinics, and hospitals, but as REMS become more common they may ultimately have a greater impact on retail-based products.

The impact of REMS is twofold. First, REMS with ETASU may require the pharmacist to verify prescriber, patient, and/or pharmacy enrollment in a registry and, in some cases, verify or check certain information, such as lab results. Second, all REMS, including those without ETASU, must fulfill FDA-approved reporting requirements. Each REMS program must also include a program assessment schedule that examines the program's effectiveness on intervals approved by the FDA as part of the overall REMS program. The results of these assessments are submitted to the FDA as part of the ongoing evaluation of REMS program effectiveness. Accordingly, we propose to include the REMS transactions as part of this proposed certification criterion. We would also note for commenters' benefit that the SCRIPT 2017071 testing tool under development is being designed to support testing these REMS transactions.

We believe that removing the 2015 Edition certification criterion (codified in § 170.315(b)(3)) that references NCPDP SCRIPT version 10.6 and replacing it with an updated e-prescribing criterion (proposed to be codified in § 170.315(b)(11)) would harmonize with relevant CMS program timelines, including Part D e-prescribing requirements and the option for eligible clinicians, hospitals, and CAHs to report on the Query of Prescription Drug Monitoring Program (PDMP) quality measure for Promoting Interoperability Programs. However, should our proposal to adopt the new e-prescribing criterion (§ 170.315(b)(11)) be finalized prior to January 1, 2020, we also propose to permit continued certification to the current 2015 Edition ''electronic prescribing'' criterion (§ 170.315(b)(3)) for the period of time in which it would continue to be used as a program standard in the CMS Medicare Part D Program or the CMS Promoting Interoperability Programs. Once it is no longer used in those Programs, we would no longer permit certification to that criterion and would remove it from the Code of Federal Regulations. We will consider setting an effective date for such actions in a subsequent final rule based on stakeholder feedback and CMS policies at the time. To this point, we note that the continued acceptability of a Health IT Module certified to the criterion codified in § 170.315(b)(3) for purposes of meeting the CEHRT definition and participating in the CMS Promoting Interoperability Programs would be a matter of CMS policy.

3. Clinical Quality Measures—Report Criterion

In the 2015 Edition final rule, ONC adopted four clinical quality measure (CQM) certification criteria, § 170.315(c)(1) CQMs—record and export, § 170.315(c)(2) CQMs—import and calculate, § 170.315(c)(3) CQMs—report, and § 170.315(c)(4) CQMs—filter (80 FR 62649–62655). These four criteria were adopted with the intent to support providers' quality improvement activities and in electronically generating CQM reports for reporting with certified health IT to programs such as the EHR Incentive Programs, Quality Payment Program, and Comprehensive Primary Care plus initiative. All four CQM criteria require certified health IT to be capable of generating CQM reports using the HL7 Quality Reporting Document Architecture (QRDA) Category I standard, which provides CQM reports for individual patients. Specifically, we adopted HL7 CDA® Release 2 Implementation Guide for: Quality Reporting Document Architecture—Category I (QRDA I); Release 1, Draft Standard for Trial Use (DSTU) Release 3 (US Realm)), Volume 1 (§ 170.205(h)(2)). Two of the CQM criteria, CQMs—report (§ 170.315(c)(3)) and CQMs—filter (§ 170.315(c)(4)), also require certified health IT to be capable of generating CQM reports using the QRDA Category III standard, which provides aggregate CQM reports for a set of patients. More specifically, we adopted QRDA Category III, Implementation Guide for CDA Release 2 (§ 170.205(k)(1)) and the Errata to the HL7 Implementation Guide for CDA® Release 2: QRDA Category III, DSTU Release 1 (US Realm), September 2014 (§ 170.205(k)(2)).

The ''CQMs—report'' certification criterion (§ 170.315(c)(3)) includes an optional certification provision for demonstrating that the health IT can create QRDA reports in the form and manner required for submission to CMS programs, which is in accordance with CMS' QRDA Implementation Guide (IGs).[23] The CMS QRDA IGs include specific requirements to support providers participating in CMS programs in addition to the HL7 IGs. At the time of the finalization of the 2015 Edition final rule and in response to public comment, we noted that there was mixed feedback on whether this criterion should require adherence to the HL7 QRDA Category I and Category III standards or solely to the CMS QRDA IGs. As such, we adopted an approach that allowed for flexibility and only required that certified health IT support the HL7 QRDA standards, which are program-agnostic and can support a number of use cases for exchanging CQM data. Because the criterion has the optional provision for CMS program-specific certification, developers can also support their end-users who intend to use their certified health IT to report eCQMs to CMS in the ''form and manner'' CMS requires (*i.e.,* using the format specified in the CMS QRDA IGs) (80 FR 62652).

Since the 2015 Edition final rule was published (October 16, 2015), we have gained additional certification experience and received feedback from the industry that health IT certified to the ''CQMs-report'' criterion (§ 170.315(c)(3)) are only/primarily being used to submit eCQMs to CMS for participation in CMS programs. Therefore, as a means of reducing burden, we propose to remove the HL7 QRDA standard requirements from the 2015 Edition CQMs—report criterion in § 170.315(c)(3), but *require* that health IT certified to the criterion support the CMS QRDA IGs. This would directly reduce burden on health IT developers and indirectly providers as they would no longer have to, in practice, develop (health IT developers) and support (both developers and providers) two forms of the QRDA standard (*i.e.,* the HL7 and CMS forms). We note that the Fast Health Interoperability Resources (FHIR) standard offers the potential for supporting quality improvement and reporting needs and promises to be a more efficient, modular, and interoperable standard to develop, implement, and utilize through APIs. However, until the potential benefits of FHIR APIs can be realized for quality improvement and reporting, we believe that solely requiring the CMS QRDA IGs for the ''CQMs—report'' criterion balances the burden to developers and providers, while still meeting the goal of facilitating quality improvement and reporting to CMS.

To support the proposal, we propose to incorporate by reference the latest annual CMS QRDA IGs, specifically the 2019 CMS QRDA I Implementation Guide for Hospital Quality Reporting[24] and the 2019 CMS QRDA III Implementation Guide for Eligible Professionals (EPs) and Eligible Clinicians.[25] A Health IT Module would need to be certified to both standards to provide flexibility to providers. However, we solicit comment on whether we should consider an approach that permits certification to only one of the standards depending on the care setting for which the product is designed and implemented. We also solicit comment on the future possibility of FHIR-enabled APIs replacing or complementing QRDA reports for quality reporting and improvement.

If we finalize this proposal in a subsequent final rule, we propose to adopt the latest CMS QRDA IGs at the time of final rule publication, as CMS updates their QRDA IGs annually to support the latest eCQM specifications and only accepts eCQM reporting to the latest version.

We note that this approach would also facilitate a means for ONC to permit developers to update its certified health IT to newer versions of the CMS QRDA IGs through the real world testing Maintenance of Certification provision for standards and implementation specification updates in support of ongoing interoperability (*see* section VII.B.5 of this proposed rule).

4. Electronic Health Information Export

We propose to adopt a new 2015 Edition certification criterion for EHI export in § 170.315(b)(10). This criterion is intended to provide patients and health IT users with a means to efficiently export the entire electronic health record for a single patient or all patients in a computable, electronic format, and facilitate the receiving health IT system's interpretation and use of the EHI, to the extent reasonably practicable using the developer's existing technology.

This outcome would promote access, exchange, and use of EHI and facilitate health care providers' ability to switch health IT systems or to migrate EHI for use in other technologies. Additionally, as discussed in section VII.B.2 of this preamble, certification to this criterion would provide some degree of assurance that a health IT developer supports, and does not inhibit, the access, exchange, and use of EHI for the specific use cases that the criterion addresses.

This proposed criterion supports two specific use cases for which we believe that all EHI produced and electronically managed in a developer's technology should be made readily available for export as a standard capability of certified health IT.

First, we propose that health IT certified to this criterion would have to enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient's behalf. This patient-focused export capability, which is discussed in more detail below, complements other provisions of this proposed rule that support patients' access to their EHI including information that may eventually be

[23] *https://ecqi.healthit.gov/qrda-quality-reporting-document-architecture.*

[24] *https://ecqi.healthit.gov/system/files/QRDA_HQR_2019_CMS_IG_final_508.pdf.*

[25] *https://ecqi.healthit.gov/system/files/2019_CMS_QRDA_III_Eligible_Clinicians_and_EP_IG-508.pdf.*

accessible via the APIs described in section VII.B.4 of this preamble. Ultimately, we expect all data to be transferred through APIs or other advanced technologies. EHI export also supports longitudinal data record development, and aligns with section 4006(a) of the Cures Act, which requires [t]he Secretary, in consultation with the National Coordinator, [to] promote policies that ensure that a patient's EHI is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient's health care providers and other individuals, including researchers, consistent with such patient's consent.

Second, this criterion would support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system. As discussed in section VIII.C.5.c.iii of this preamble, health IT developers are in a unique position to block the export and portability of data for use in competing systems or applications, or to charge rents for access to the basic technical information needed to facilitate the conversion or migration of data for these purposes. By providing at least a baseline capability for exporting EHI in a commercially reasonable format, we believe that this criterion would help to address some of these business practices and enable smoother transitions between health IT systems.

This criterion is intended to further the two use cases outlined above while providing an incremental approach given the known and anticipated health IT landscape when ONC expects certified health IT with this functionality will be widely available in the ecosystem. At the time of this rulemaking, we believe a focused certification criterion that is standards-agnostic will provide a useful first step to enabling patients to request and receive their EHI and for providers to more readily switch or migrate information between health IT systems. Understanding that open, standards-based APIs are an emerging technology and that some health IT developers today have implemented proprietary APIs, this proposed criterion for EHI export provides an initial method for exporting patient health information in these circumstances. Over time, ONC may consider expanding the proposed criterion or replacing it to achieve the goals in § 170.402. It is also possible that in the future, this criterion will no longer be needed once standards-based APIs are widely available in the health IT ecosystem with the ability to facilitate exchange of a wider set of standardized data elements per the predictable, transparent, and collaborative process to expand the USCDI (*see* the discussion of the API Condition of Certification and the proposed API criterion in § 170.315(g)(10) in VII.B.4 for additional information).

a. Patient Access

As noted above, the export functionality required by this certification criterion would support both a patient's access to their EHI and a provider's ability to switch to another health IT system. In the patient access context, we propose that a user must be able to timely execute the single patient EHI export at any time the user chooses and without subsequent developer assistance to operate. The health IT developer should enable the user to make data requests and receive the export efficiently, without unreasonable burden. For example, the health IT developer should not: Require the user to make a request multiple times for different types of EHI; provide unreasonable delays for the export; or prohibit reasonable user access to the system during the export process.

''Timely'' does not mean real-time; however, we stress that any delays in providing the export must be no longer than reasonably necessary to avoid interference with other clinical functions of the health IT system. This is similar to the approach we have taken for export of clinical quality measure data. The export capability does not require that data be received instantaneously. Rather, as we have stated before (80 FR 62650) a non-conformity would exist if surveillance revealed that processing or other delays were likely to substantially interfere with the ability of a provider or health system to view and verify their CQM results for quality improvement on a near real-time basis. Similarly, a non-conformity would exist if delays were causing or contributing to users being presented with data files that no longer contained current, accurate, or valid data. To avoid these implementation issues and ensure that capabilities support all required outcomes, health IT developers should seek to minimize processing times and other delays to the greatest extent possible.[26]

As previously defined under the Program, ''user'' is a health care professional or his or her office staff; or a software program or service that would interact directly with the certified health IT (80 FR 62611, 77 FR 54168). We typically would expect the ''user'' in this case to be a provider or his or her office staff who will be performing the request on behalf of the patient given that a request of this nature would likely occur in the context of an individual exercising their right of access under the HIPAA Privacy Rule (45 CFR 164.524). In this regard, the proposed 2015 Edition ''EHI export'' criterion could facilitate and support the provision of a patient's record in an electronic format. In service to innovative and patient-centric approaches, a health IT developer could develop a method that allows the patient using a technology application (*e.g.,* portal or ''app'') to execute the request without needing a provider to do so on their behalf. We seek comment on whether this portion of the criterion should be made more prescriptive to *only* allow the patient and his or her authorized representative to be the requestor of their EHI, similar to how we have previously scoped such criteria as ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1)).

Similar to the 2015 Edition ''data export'' certification criterion (§ 170.315(b)(6)), which we propose for removal below, we acknowledge potential privacy and security concerns may arise when EHI is exported and, therefore, propose that for provider-mediated requests, a developer may design the health IT to limit the type of users that would be able to access and initiate EHI export functions. However, as we previously specified in the 2015 Edition final rule, the ability to ''limit'' the single patient EHI export functionality is intended to be used by and at the discretion of the provider organization implementing the technology, not a way for health IT developers to implicitly prevent the overarching user-driven aspect of this capability (80 FR 62646).

b. Transitions Between Health IT Systems

In addition to and separate from the patient access use case described above, health IT certified to this criterion would facilitate the migration of EHI to another health IT system. We propose that a health IT developer of health IT certified to this criterion must, at a customer's request, provide a complete export of all EHI that is produced or managed by means of the developer's certified health IT. Health IT developers would have flexibility as to how this outcome is achieved, so long as a customer is able to receive the export in a timely and efficient manner, and in a format that is commercially reasonable. For example, in contrast with the patient export capability, which must be available to a user without subsequent

[26] *https://www.healthit.gov/test-method/clinical-quality-measures-cqms-record-and-export#ccg.*

developer assistance to operate, the ''database export'' capability of this criterion could require action or support on the part of the health IT developer.

We note that while this criterion focuses on the technical outcomes supported by this capability, developers of health IT certified to this criterion would be required to provide the assurances proposed in § 170.402, which include providing reasonable cooperation and assistance to other persons (including customers, users, and third-party developers) to enable the use of interoperable products and services. Thus, while developers would have flexibility as to how they implement the export functionality for transitions between systems, they would ultimately be responsible for ensuring that the capability is deployed in a way that enables a customer and their third-party contractors to successfully migrate data. Such cooperation and assistance could include, for example, assisting a customer's third-party developer to automate the export of EHI to other systems. We refer readers to section VII.B.2 of the proposed rule for further discussion of a health IT developer's assurances as proposed in § 170.402.

c. Scope of EHI

For both use cases supported by this criterion, EHI export encompasses all the EHI that the health IT system produces and electronically manages for a patient or group of patients. This applies to the health IT's entire database, including but not limited to clinical, administrative, and claims/billing data. It would also include any data that may be stored in separate data warehouses that the system has access to, can produce, and electronically manages. For example, health IT developers may store EHI in these warehouses to prevent performance impacts from data queries that may slow down the ''main'' health IT system's (*e.g.,* EHR) clinical performance. We clarify that ''EHI'' also includes the oldest EHI available on that patient to the most recent, no matter the specific electronic format (*e.g.,* PDFs are included). As mentioned above, our intention is that ''produces and electronically manages'' refers to a health IT product's entire database. However, we seek comment on the terminology used (''produces and electronically manages'') and whether that captures our intent or whether there are any alternatives to the language we should consider to further clarify our intent. Alternative language we considered included ''produce and electronically retain'' data, which could encompass more data.

The use of the term ''electronic health information'' (EHI) is deliberate and in alignment with the Cures Act and the proposed definition of this term in § 170.102. Its use supports consistency and the breadth of types of data envisioned by this criterion. Clinical data would encompass imaging information—both images and narrative text about the image—as this is part of the patient's total record; however, we understand that EHRs may not be the standard storage location for images and solicit comment on the feasibility, practicality, and necessity of exporting images and/or imaging information. We request comment on what image elements, at a minimum, should be shared such as image quality, type, and narrative text. It is understandable that developers will not be able to export every existing data element, nor that all possible data elements are necessary for transfer. For finalization in a subsequent final rule, we solicit comment on whether we should require, to support transparency, health IT developers to attest or publish as part of the export format documentation the types of EHI they cannot support for export.

We also propose the following metadata categories that would be excluded from this criterion, and have listed examples for clarity below. We seek comment on these exclusion categories, and request feedback on what metadata elements should remain included for export, or be added to the list of data that would be allowed to be excluded in a subsequent final rule:

- Metadata present in internal databases used for physically storing the data. Examples include: Internal database table names, field names, schema, constraints, Triggers, Field size (number of bytes), Field type (String, integer, double, long), and Primary keys or object identifiers used internally for querying.
- Metadata that may not be necessary to interpret EHI export, including information that is typically required for processing of transactions such as encryption keys, internal user roles, ancillary information such as information stored in different formats, local codes for internal use; audit logs, record reviews, or history of change.
- Metadata that refers to data that is not present in the EHI export, such as links to files and other external attachments that are not part of the export, and information used in conjunction with data from other applications that is not part of the health IT.

We also seek comment, for consideration in finalizing this criterion in a subsequent final rule, on types of EHI that may present challenges for meeting the intent of this proposed criterion.

d. Export Format

The proposed certification criterion does not prescribe a content standard for the EHI export. However, it requires health IT developers to provide the format, such as a data dictionary or export support file, for the exported information to assist the receiving system in processing the EHI without loss of information or its meaning to the extent reasonably practicable using the developer's existing technology. Providing EHI export information is consistent with emerging industry practices and capabilities to offer requestors the ability to access, download, and move their information without unreasonable burden. Companies such as Facebook,[27] Google,[28] and Twitter [29] offer publicly-available links which provide requestors necessary information on how to download their personal information including, in some cases, several download options for requestors alongside their export instructions. Public access to comparable EHI export information would further support third-party companies in this space, as they would have additional information and general knowledge for use of available data. Accordingly, we propose that the developer's export format should be made publicly available via a hyperlink as part of certification to the ''EHI export'' criterion, including keeping the hyperlink up-to-date with the current export format.

We believe that by making the export format publicly available at the time of certification (and keeping the information current) will stimulate a vibrant, competitive market in which third- party software developers can specialize in processing the data exported from certified health IT products in support of patients and providers. Moreover, we believe this proposal will transform today's current guess-work, one-off processes into something more predictable and transparent such that greater industry efficiencies can be realized. We note and clarify that the export format need not be the same format used internally by the health IT system, and the health IT developer would not need to make public their proprietary data model. The proposed certification criterion also

[27] *https://www.facebook.com/help/1701730696756992?helpref=hc_global_nav.*

[28] *https://support.google.com/accounts/answer/3024190?hl=en.*

[29] *https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive.*

does not prescribe how the exported EHI is made available to the user, as this may depend on the size and type of information. We would expect that the information be made available to the user or requestor in an acceptable manner without placing unreasonable burden on the user or requestor. Please also generally see our discussion of information blocking in section VIII and particularly section VIII.D.5.

e. Initial Step To Persistent Access to All of a Patient's EHI

We believe that open, standards-based APIs should provide persistent access to patients' EHI over time to achieve the envisioned goals in § 170.404. In the meantime, this proposed criterion in § 170.315(b)(10) will provide an initial step toward achieving those goals. We clarify that ''persistent'' or ''continuous'' access to EHI is not required to satisfy this criterion's requirements and that the minimum requirement is for a discrete data export capability. Similarly, while the criterion requires the timely export of all EHI, such export need not occur instantaneously (or in ''real-time''). However, health IT developers are encouraged to consider persistent access and real-time approaches as part of the step-wise progression we see towards open, standards-based APIs for a growing number of data elements per the USCDI in the proposed ''standardized API for patient and population services'' criterion (§ 170.315(g)(10).'' Further, we caution that where it is reasonable for a developer to provide persistent or real-time access to electronic health information, the refusal to do so may be inconsistent with the Conditions of Certification in § 170.401 (information blocking) and § 170.402 (assurances related to this capability), as well as the information blocking provision, as to which readers should refer to sections VII and VIII of this proposed rule. Similarly, while this certification criterion would provide a baseline capability for exporting data for the specific use cases described above, health IT developers may need to provide other data export and conversion services or support additional export use cases beyond those encompassed by this criterion to facilitate the appropriate access, exchange, and use of electronic health information and to avoid engaging in information blocking.

f. Timeframes

ONC seeks input on EHI export and timeframes. In particular, beyond exporting *all* the EHI the health IT system produces and electronically manages, should this criterion include capabilities to permit health care providers to set timeframes for EHI export, such as only the ''past two years'' or ''past month'' of EHI?

For discussion of the required timeframe for developers of certified health IT *to certify to this proposed criterion and make it available to their customers,* please see Section VII.B.2, which addresses a health IT developer's required assurances regarding the availability and provision of this EHI export capability to its customers.

g. Replaces the 2015 Edition ''Data Export'' Criterion in the 2015 Edition Base EHR Definition

We propose to remove the ''data export'' criterion (§ 170.315(b)(6)) from the 2015 Edition, including the 2015 Edition Base EHR definition expressed in § 170.102. Correspondingly, we propose to include the proposed ''EHI export'' criterion (§ 170.315(b)(10)) in the 2015 Edition Base EHR definition, which would affect health care providers' compliance responsibilities when it comes to possessing CEHRT for associated CMS programs. A specific C–CDA data export criterion no longer supports advancements in interoperability in the evolving health IT industry. The proposed ''EHI export'' certification criterion is standards-agnostic and supports a more open approach to interoperability. More specifically, the proposed ''EHI export'' criterion differs significantly from the ''data export'' certification criterion as the latter is limited to clinical data as specified in the C–CDA. Also, the proposed ''EHI export'' criterion is not limited to just the scope of the certified capabilities in the certified Health IT Module as it applies to all produced and electronically managed EHI. Further, by including this functionality in the 2015 Base EHR definition, we can be assured that health care providers participating in the CMS programs (*e.g.,* Promoting Interoperability Programs) have functionality to both support patient requests for their EHI and switching health IT systems.

We propose to modify the Base EHR definition to include the proposed ''EHI export'' criterion 24 months from the effective date of the final rule for this proposed rule (which practically speaking would be 25 months because of the 30-day delayed effective date). We believe this is sufficient time for health IT developers to develop, test, certify, and rollout this functionality to health care providers based on the flexible approach offered for meeting this criterion. We also believe this timeframe provides sufficient time for health care providers to adopt and implement the functionality included in the ''EHI export'' criterion. To note, we refer readers to the ''Assurances'' Condition and Maintenance of Certification requirements in section VII.B.2, which propose complementary requirements on health IT developers to rollout health IT certified ''EHI export'' within 24 months of the effective date of a final rule for this proposed rule. We welcome comments on our proposed compliance timeline.

We note that we do not propose a transition period for the ''data export'' criterion. We propose to remove the criterion from the 2015 Edition upon the effective date of a final rule for this proposed rule. Unlike the ''application access—data category request'' criterion (which we propose to replace with the new API criterion in this proposed rule), the ''data export'' criterion does not support an objective or measure under the CMS Promoting Interoperability Programs. Therefore, we do not believe that health IT developers and health care providers need to support the functionality in the ''data export'' criterion while they transition to the development, adoption, and implementation of the EHI export criterion. This approach should reduce burden and costs for both health IT developers and health care providers. We welcome comments on this approach, including whether this will leave health care providers without an export capability for an inordinate period of time such that we should require health IT developers to support the ''data export'' functionality for health care providers until the health IT developer attests to providing the new EHI export functionality to all of its customers.

Readers are also referred to the Regulatory Impact Analysis in section XIV of this proposed rule for a discussion of the estimated costs and benefits of this proposed criterion, as well as the impact of the proposed removal of the 2015 Edition ''data export'' criterion.

5. Standardized API for Patient and Population Services Criterion

To implement the Cures Act, we propose to adopt a new API criterion in § 170.315(g)(10), which would replace the ''application access—data category request'' certification criterion (§ 170.315(g)(8)) and become part of the 2015 Edition Base EHR definition. This new certification criterion would require the use of FHIR standards, several implementation specifications, and focus on supporting two types of API-enabled services: (1) Services for which a single patient's data is at focus; and (2) services for which multiple patients' data are at focus. Please refer to the ''Application Programming Interfaces'' section (VII.B.4) in this preamble for a more detailed discussion of the ''API'' certification criterion and related Conditions and Maintenance of Certification requirements.

6. Privacy and Security Transparency Attestations

a. Background

In 2015, the HIT Standards Committee (HITSC) recommended the adoption of two new certification criteria for the Program. The National Coordinator endorsed the HITSC recommendations for consideration by the Secretary, and the Secretary determined that it was appropriate to propose adoption of the two new certification criteria through rulemaking (81 FR 10635). To implement the Secretary's determination, we propose to add two new 2015 Edition privacy and security ''transparency attestation'' certification criteria for: (1) Encrypt authentication credentials; and (2) multi-factor authentication.

In the 2015 Edition final rule, we adopted a new, simpler, and straightforward approach to privacy and security (P&S) certification requirements for Health IT Modules certified to the 2015 Edition, which we refer to as the 2015 Edition privacy and security certification framework (80 FR 62705). In this proposed rule, we propose modifications to the 2015 Edition privacy and security certification framework in § 170.550(h) and propose to add new criteria to which a health IT developer would need to certify pertaining to whether or not its product encrypts authentication credentials (specifically § 170.315(d)(12)) and supports multi-factor authentication (specifically § 170.315(d)(13)). To be clear, we are not proposing to require that health IT *have* the functionality present to encrypt authentication credentials or support multi-factor authentication. Rather, we propose that a health IT developer indicate whether or not their certified health IT has those capabilities by attesting yes or no.

b. Encrypt Authentication Credentials

We propose to adopt an ''encrypt authentication credentials'' certification criterion in § 170.315(d)(12) and include it in the P&S certification framework (§ 170.550(h)). We propose to make the encrypt authentication credentials certification criterion applicable to any Health IT Module currently certified to the 2015 Edition and any Health IT Module presented for certification due to the fact that all health IT must meet the ''authentication, access control, and authorization'' certification criterion adopted in § 170.315(d)(1) as part of current Program requirements. While the 2015 Edition ''authentication, access control, and authorization'' certification criterion criteria requires that patient information saved on end user devices is encrypted, those same protections are not explicitly required through certification for the authentication credentials used to access that same information. As such, we believe that this proposal would address that gap and encourage health IT developers to take steps to ensure that authentication credentials are protected consistent with industry best practices.

To provide clarity as to what a ''yes'' attestation for ''encrypt authentication credentials'' would mean, we provide the following explanation. Encrypting authentication credentials could include password encryption or cryptographic hashing, which is storing only encrypted or cryptographically hashed passwords. If a developer attests that its Health IT Module encrypts authentication credentials, we propose that the attestation would mean that the Health IT Module is capable of cryptographically protecting stored authentication credentials in accordance with standards adopted in § 170.210(a)(2), Annex A: Federal Information Processing Standards (FIPS) Publication 140–2, Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules. We posit that FIPS Publication 140–2 is the seminal, comprehensive, and most appropriate standard. Moreover, in the specified FIPS 140–2 standard, there is an allowance for various approved encryption methods, and health IT developers would have the flexibility to implement any of the approved encryption methods in order to attest yes to this criterion. Health IT developers should keep apprised of these standards as they evolve and are updated to address vulnerabilities identified in the current standard.

We do not believe it is necessary for a Health IT Module to be required to be tested to this criterion, so long as by attesting yes to this criterion, the health IT developer is attesting that if authentication credentials are stored, then the authentication credentials are protected consistent with the requirements above. To be clear, a ''no'' attestation is a sufficient response to address this certification criterion; however, health IT developers should be aware that this ''no'' will be made publicly available on the CHPL. Note that if a developer attested to encrypting authentication credentials, a certified Health IT Module would be subject to ONC–ACB surveillance for any potential non-conformity with the requirements of this criterion. Specifically, if the ONC–ACB becomes aware of situations where the developer's health IT is not meeting the developer's affirmative attestation per the criterion's requirements, the ONC–ACB may use its corrective action process to bring the product back into conformance.

We propose that, for health IT certified prior to a subsequent final rule's effective date, the health IT would need to be certified to the ''encrypt authentication credentials'' certification criterion within six months after the final rule's effective date. For health IT certified for the first time after the final rule's effective date, we propose that the health IT must meet this criterion at the time of certification. This should allow sufficient time for health IT developers to assess their Health IT Modules' capabilities and attest ''yes'' or ''no'' to the certification criterion.

For an assessment of this proposal's costs and benefits, please refer to the Regulatory Impact Analysis in section XIV of this preamble. We welcome comments on this assessment and this proposal in general. We also note that some health IT presented for certification is not designed to store authentication credentials. Therefore, we specifically request comment on whether we should include an explicit provision in this criterion to accommodate such health IT. This could be similar to the approach we have taken with the 2015 Edition ''end-user device encryption'' criterion (§ 170.315(d)(7)(ii)), where we permit the criterion to be met if the health IT developer indicates their technology is designed to prevent electronic health information from being locally stored on end-user devices.

c. Multi-Factor Authentication

We propose to adopt a ''multi-factor authentication'' (MFA) criterion in § 170.315(d)(13) and include it in the P&S certification framework (§ 170.550(h)). We propose to make the ''multi-factor authentication'' certification criterion applicable to any Health IT Module currently certified to the 2015 Edition and any Health IT Module presented for certification. Health IT developers have already been implementing MFA to meet the Electronic Prescribing of Controlled Substances (EPCS) requirements set by Drug Enforcement Administration (DEA), and if adopted, this certification criterion would be general in that its intended outcome would provide more public transparency around the MFA capabilities included in certified health IT.

This proposal supports the Department of Homeland Security (DHS) led initiative ''STOP, THINK, CONNECT'' which strongly recommends and runs campaigns to promote stronger authentication, typically related to MFA, going beyond a username and password to log in. MFA is also recommended by numerous organizations and groups. In the ''Report on Improving Cybersecurity in the Health Care Industry,'' [30] the Health Care Industry Cybersecurity Task Force recommended requiring strong authentication to improve identity and access management for health care workers, patients, and medical devices/EHRs. Using a single factor approach to accessing information is particularly prone to cyber-attack because one factor passwords can be weak, stolen, and are vulnerable to external phishing attacks, malware, and social engineering threats. In situations where the provider is accessing a health IT product or health information exchange external to the hospital or clinical environment, the Health Care Industry Cybersecurity Task Force recommended that the health care industry adopt the NIST SP 800–46 guidelines for remote access, including the use of two-factor authentication to ensure a compromised password cannot alone be used to gain access. Promoting the use of MFA and leveraging biometrics, mobile phones, and/or wearables can help to establish a trust relationship with the patient. Additionally, NIST recommends any personal data, whether self-asserted or validated, require MFA.

However, despite the benefits of adopting MFA, we are also aware of some of the challenges. Specifically, in health care, many providers are resistant to adopt MFA because of the inconvenience and loss of time of going through another step to access the patient's EHI. Also, MFA has not been deployed very long in the health care setting, so it is not clear how much it actually addresses the risk. In most MFA implementations, passwords are still present. In addition to having to manage passwords, users also have to manage an additional layer of security. Another usability challenge is that systems often require different types of MFA, which adds to the complexity and also may require providers to keep track of tokens. MFA is often recommended as a solution to password problems, but it is still vulnerable to theft. These alternative forms of authentication have their own set of vulnerability issues. The cost of implementing MFA and ensuring it will be implemented in a way that does not inhibit clinical workflow is also an issue to be considered.

To provide clarity as to what a ''yes'' attestation for ''multi-factor authentication'' attestation would mean, we provide the following explanation. MFA requires users to authenticate using multiple means to confirm they are who they claim to be in order to prove one's identity, under the assumption that it is unlikely that an unauthorized individual or entity will be able to succeed when more than one token is required. MFA includes using two or more of these: (i) Something people know, such as a password or a personal identification number (PIN); (ii) something people have, such as a phone, badge, card, RSA token or access key; and (iii) something people are, such as fingerprints, retina scan, heartbeat, and other biometric information. Thus, in order to be issued a certification, we propose to require that a Health IT Module developer attest to whether or not its certified health IT supports MFA consistent with industry recognized standards (*e.g.,* NIST Special Publication 800–63B Digital Authentication Guidelines, ISO 27001).

We propose that, for health IT certified prior to a subsequent final rule's effective date, the health IT would need to be certified to the ''multi-factor authentication'' certification criterion within six months after the final rule's effective date. For health IT certified for the first time after the final rule's effective date, we propose that the health IT must meet this criterion at the time of certification. This should allow sufficient time for health IT developers to assess their Health IT Modules' capabilities and attest ''yes'' or ''no'' to the certification criterion.

We generally seek comment on whether there is value in adopting the proposed ''multi- factor authentication'' criterion. We also solicit comment on the method of attestation and, if the health IT developer does attest to supporting MFA, whether we should require the health IT developer to explain how they support MFA. For example, should the health IT developer be required to identify the MFA technique(s) used/supported by submitting specific information on how it is implemented, including identifying the purpose(s)/use(s) to which MFA is applied within their Health IT Module (such as where in the clinical workflow it is required), and, as applicable, whether the MFA solution complies with industry standard? This information could enable the health IT developer to highlight their health IT's capabilities to support MFA.

7. Data Segmentation for Privacy and Consent Management Criteria

We adopted two 2015 Edition ''data segmentation for privacy'' (DS4P) certification criteria in the 2015 Edition final rule. One criterion (''DS4P-send'' (§ 170.315(b)(7)) includes capabilities for creating a summary care record formatted to the C–CDA 2.1 standard and document-level tagging as restricted (and subject to restrictions on re-disclosure) according to the DS4P standard. The other criterion (''DS4P-receive'' (§ 170.315(b)(8)) includes capabilities for receiving a summary care record formatted to the C–CDA 2.1 standard and document-level tagged as restricted (and subject to restrictions on re-disclosure) according to the DS4P standard. As noted in the 2015 Edition final rule (80 FR 62646)), certification to these criteria is not required to meet the CEHRT definition for CMS EHR Incentive Programs, now referred to as the Promoting Interoperability Programs. The current 2015 Edition DS4P certification criteria specify the technical capabilities that the health IT must have to apply and recognize security labels in a summary document (C–CDA) such that the recipient of a summary document would be able to recognize the existence of sensitive elements within the summary document (80 FR 62646). Security labeling provides a way for computer systems to properly handle data passed among systems, to preserve the condition of security, and to enable access control decisions on the information, so that the information is only accessed by the appropriate entities. The HL7 Healthcare Classification System (HCS) standard provides a common syntax and semantics for interoperable security labels in health care. The DS4P standard makes use of the HCS specification and describes a method for applying security labels to HL7 CDA documents to ensure that privacy policies established at a record's source can be understood and enforced by the recipient of the record.

In the 2015 Edition final rule, we noted that the DS4P standard is not restricted to data subject to the federal regulations governing the Confidentiality of Substance Use Disorder Patient Records (42 CFR part 2) (80 FR 62647). It may be implemented to support other data exchange use cases in which compliance with state or federal legal frameworks require sensitive health information to be tagged

[30] *https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.*

and segmented (80 FR 62647). We further stated that we offered certification to these criteria as an initial step towards the ability of an interoperable health care system to use technical standards to compute and persist security labels to permit access, use, or disclosure of protected health information in accordance with applicable policies and patient preferences. We understood and acknowledged additional challenges surrounding the prevalence of unstructured data, sensitive images, and potential issues around use of sensitive health information by clinical decision support systems. The adoption of document level data segmentation for structured documents would not solve these issues, but we acknowledged it would help move technology in the direction where these issues could be addressed (80 FR 16841).

Adoption of the current 2015 Edition DS4P criteria was also consistent with earlier HIT Policy Committee (HITPC) recommendations on the use of DS4P technology to enable the electronic implementation and management of disclosure policies that originate from the patient, the law, or an organization, in an interoperable manner, so that electronic sensitive health information may be appropriately shared.[31] These HITPC recommendations consisted of a glide path for the exchange of 42 CFR part 2-protected data starting with the inclusion of Level 1 (document level tagging) send and receive functionality. The HITPC also recommended advancing the exchange of 42 CFR part 2-protected data, by outlining additional capabilities in sharing, viewing and incorporating privacy restricted data at a more granular level, as well as managing computable patient consent for the use of restricted data.[32]

Since the 2015 Edition final rule, the health care industry has engaged in additional field testing and implementation of the DS4P standard. As of the beginning of the third quarter of the 2018 CY, only about 20 products (products with multiple certified versions were counted once) were certified to the current 2015 Edition DS4P certification criteria. In addition, stakeholders shared with ONC—through public forums, listening sessions, and correspondence—that focusing certification on segmentation to only the document level does not permit providers the flexibility to address more granular segmentation needs. Stakeholders noted that certain provider types, such as providers of pediatric care and behavioral health care, are currently using a range of burdensome manual workflows in order to meet complex use cases for DS4P which are also impacted by state and local laws. Additionally, stakeholders have expressed interest in ONC exploring health IT standards that work with DS4P to support the management of consent for sharing documents that include security labels such as through the use of an API.

Therefore, in consideration of stakeholder feedback and our stated policy approach to adopt DS4P certification criteria on a glide path, we propose to remove the current 2015 Edition DS4P-send (§ 170.315(b)(7)) and DS4P-receive (§ 170.315(b)(8)) certification criteria. The proposed effective date of removal of these criteria would be the effective date of a subsequent final rule for this proposed rule. We propose to replace these two criteria with three new 2015 Edition DS4P certification criteria (two for C–CDA and one for a FHIR-based API) that would support a more granular approach to privacy tagging data and consent management for health information exchange supported by either the C–CDA– or FHIR-based exchange standards. Our primary purpose for proposing to remove and replace them, in lieu of proposing to revise them, is to provide clarity to stakeholders as to the additional functionality enabled by health IT certified to the new criteria. We note resources released by ONC and OCR, such as the HHS Security Risk Assessment Tool[33] and the Guide to Privacy and Security of Electronic Health Information,[34] as well as the Office for Civil Rights' security risk analysis guidance[35] that entities may employ to make risk-based decisions regarding their implementation of the proposed DS4P criteria. We also note the availability of the Electronic Consent Management Landscape Assessment, Challenges, and Technology report.[36] The report includes suggestions for overcoming barriers associated with implementing electronic consent management, which may be considered for further research and discussion.

a. Implementation With the Consolidated CDA Release 2.1

In place of the removed 2015 Edition DS4P criteria, we propose to adopt new DS4P-send (§ 170.315(b)(12)) and DS4P-receive (§ 170.315(b)(13)) criteria that would remain based on the C–CDA and the HL7 DS4P standard. These criteria would include capabilities for applying the DS4P standard at the document, section, and entry level. We believe this offers more valuable functionality to providers and patients, especially given the complexities of the landscape of privacy laws for multiple care and specialty settings. We believe health IT certified to these criteria could support multiple practice settings and use cases. For example, in section VI.A.2 of this preamble, we explain how the proposed capabilities included in these criteria could support the pediatric health care setting. We believe this proposal could also reduce burden for providers by leveraging health IT's ability to recognize and manage sensitive data and patient consent directives, rather than relying on case-by-case manual redaction and subsequent workarounds to transmit redacted documents. We emphasize that health care providers already have processes and workflows to address their existing compliance obligations which could be made more efficient and cost effective through the use of health IT. We recognize that more granular privacy markings at the point of data capture would further support existing and future priorities of states for multiple care and specialty settings, including behavioral health and pediatric health care settings.

We welcome public comment on our proposals to replace the current 2015 Edition DS4P criteria and adopt new 2015 Edition DS4P-send (§ 170.315(b)(12)) and DS4P-receive (§ 170.315(b)(13)) criteria to support improved options for data segmentation for health care providers engaged in complex use cases such as those identified in pediatric care (*see also* section VI.A) and behavioral health

[31] See HIT Policy Committee (HITPC) Recommendation Letter to ONC, July 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf;* see also HITPC's Privacy and Security Tiger Team Public Meeting, Transcript, May 12, 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-12.pdf;* Public Meeting, Transcript, May 27, 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-27.pdf.*

[32] For more details on the two glide paths for part 2-protected data, see *http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf.*

[33] HHS Security Risk Assessment Tool: *http://www.healthit.gov/providers-professionals/security-risk-assessment.*

[34] ONC Guide to Privacy and Security of Electronic Health Information: *http://www.healthit.gov/sites/default/files/ pdf/privacy/privacy-and-security-guide.pdf.*

[35] HHS Office for Civil Rights:*https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html;* and *https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.*

[36] *https://www.healthit.gov/sites/default/files/privacy-security/ecm_finalreport_forrelease62415.pdf.*

care, including for opioid use disorder (OUD) (*see also* section VI.B).

b. Implementation With FHIR Standard

In collaboration with ONC, the Substance Abuse and Mental Health Services Administration (SAMHSA) developed the Consent2Share application to address the specific privacy protections of patients with substance use disorders who are covered by the federal confidentiality regulation, 42 CFR part 2. Consent2Share is an open source application for data segmentation and consent management. It is designed to integrate with existing FHIR systems. SAMHSA created a FHIR implementation guide (the Consent2Share Consent Profile Design, hereafter referred to as ''Consent Implementation Guide'') that describes how the Consent2Share (C2S) application and associated access control solution uses the FHIR Consent resource to represent and persist patient consent for treatment, research, or disclosure.[37] The implementation guide provides instructions for using the FHIR Consent resource to capture a record of a health care consumer's privacy preferences.

As discussed in section VII.B.4 of this proposed rule, we are proposing policies related to the implementation of a standardized API to support the exchange of health information between providers and patients and among members of a care team. We anticipate that the proposed 2015 Edition ''standardized API for patient and population services'' certification criterion (§ 170.315(g)(10)) will result in a proliferation of APIs that will enable a more flexible and less burdensome approach to exchanging EHI. We believe the health care industry can leverage this API infrastructure to share segmented data in a secure and scalable manner. Therefore, we propose to adopt a 2015 Edition certification criterion ''consent management for APIs'' in § 170.315(g)(11) to support data segmentation and consent management through an API in accordance with the Consent Implementation Guide. Certification to this criterion would be at a health IT developer's discretion and would indicate that a system is capable of responding to requests through an API for patient consent directives that include standards-based security labeling.

We acknowledge that our proposed implementation specification, the Consent Implementation Guide, is based on a different version of the FHIR standard (FHIR Standard for Trial Use 3, also known as FHIR Release 3) than the proposed ''standardized API for patient and population services'' criteria (§ 170.315(g)(10)) which is proposed to reference just FHIR Release 2. Furthermore, we acknowledge that this discrepancy may result in additional implementation efforts for developers. In ideal circumstances, we would have proposed a data segmentation and consent management standard for APIs that was based on FHIR Release 2 and aligned with the ''standardized API for patient and population services'' criteria proposed in this proposed rule. However, although SAMHSA also created a consent implementation guide based on FHIR Release 2,[38] the guide used the FHIR ''Contract'' resource to represent patient consent directives. It is our understanding that an approach based on the ''Contract'' resource has since been abandoned by the industry in favor of using the ''Consent'' resource which was introduced in FHIR Release 3. Moreover, the FHIR Release 2 version of the Consent Implementation Guide went through relatively little testing and was never formally implemented because SAMHSA began developing an update to the guide based on the ''Consent'' resource in FHIR Release 3. Consequently, proposing an implementation specification based on FHIR Release 2 would not have aligned with the more common implementation of FHIR-based consent directives by the health care industry. We do not anticipate that the initial misalignment between the proposed API criterion (§ 170.315(g)(10)) and the proposed third DS4P criterion (§ 170.315(g)(11)) will pose a significant burden on health IT developers. Further, our proposal to permit health IT developers to voluntarily implement and use a new version of an adopted standard or implementation specification so long as such version was approved by the National Coordinator for use in certification through the Standards Version Advancement Process, discussed in section VII.B.5, would enable standards version alignment between these two criteria in the future as the FHIR standard matures.

SAMHSA created the ''Consent Implementation Guide'' to support developers in implementing the FHIR Consent resource to represent patient consent for treatment, research, and disclosure. The Consent Implementation Guide provides instructions for using the FHIR ''Consent'' resource to capture a record of a health care consumer's privacy preferences. Implementing an instance of the FHIR Consent resource based on this guide allows for a patient consent to permit or deny identified recipient(s) or recipient role(s) to perform one or more actions, regarding the patient's health information for specific purposes and periods of time. For example the Consent Implementation Guide supports consent management for specific use cases to permit or deny disclosure based on a specific law, regulation, or policy under which the patient consented. The implementation guide uses security labels as a mechanism for specifying a patient's preferences (*e.g.,* permit disclosure of EHI labeled ''restricted''). The Consent Implementation Guide provides a much simpler mechanism for representing a patient's consent preferences than the old approach based on FHIR Release 2 and has undergone implementation and pilot testing by SAMHSA's Consent2Share (C2S) application.

Our proposal to adopt the version aligned with FHIR Release 3 and the FHIR Release 3 standard for this criterion reflects stakeholder interests and efforts to support particular use cases. C2S enables data segmentation and consent management for disclosure of several discrete categories of sensitive health data related to conditions and treatments including: Alcohol, tobacco and substance use disorders (including opioid use disorder), behavioral health, HIV/AIDS, and sexuality and reproductive health. These capabilities support multiple use cases in both primary and specialty care, and specifically address priority needs identified by stakeholders to support pediatric care. We emphasize that health care providers already have processes and workflows to address their existing compliance obligations which could be made more efficient and cost effective through the use of health IT. Finally, given that the FHIR standard is modular in nature, and especially since the ''Consent'' resource did not exist in FHIR Release 2, we anticipate that health IT developers that elect to certify to this criterion would be able to support the Consent Implementation Guide along with the API requirements specified in ''standardized API for

[37] The draft FHIR IG titled ''*Consent2Share FHIR Profile Design.docx*'' can be accessed through the Community- Based Care and Privacy (CBCP) HL7 workgroup, within the Package Name titled ''*BHITS_FHIR_Consent_IG,*'' at *https://gforge.hl7.org/gf/project/cbcc/frs/.*

[38] The draft Behavioral Health Information Technologies and Standards (BHITS) FHIR DSTU2 Consent Implementation Guide can be accessed through the Community-Based Care and Privacy (CBCP) HL7 workgroup at *https://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseView&release_id=1279.*

patient and population services'' (§ 170.315(g)(10)) with modest extra effort.

We welcome comments on this proposal. We specifically seek comment on how the availability of this proposed certification criterion might increase the ability to support multiple care coordination and privacy priorities, including those associated with pediatric care; and whether we should consider other similar API based options and resources as standards for certification criteria. We also seek comment on whether the misalignment between the versions of the FHIR standard used by our proposed ''consent management for APIs'' and ''standardized API for patient and population services'' criteria would create excessive burden for developers and implementers. Specifically, we seek comment on if certification to the ''consent management for APIs'' should only be available in conjunction with the ''standardized API for patient and population services'' criteria at such a time as the criteria are aligned to one version of the FHIR standard or if the option to certify to the ''consent management for APIs'' should be allowed for those developers interested in doing so even without current standards alignment. We note that SAMHSA is currently pursuing additional work to expand use cases related to data segmentation for privacy and FHIR compatibility.

C. Unchanged 2015 Edition Criteria—Program Reference Alignment

In the FY 2019 IPPS/LTCH PPS proposed rule (83 FR 20516), CMS proposed scoring and measurement policies to move beyond the three stages of meaningful use to a new phase of EHR measurement with an increased focus on interoperability and improving patient access to health information. To reflect this focus, CMS changed the name of the Medicare and Medicaid EHR Incentive Programs, to the Medicare and Medicaid Promoting Interoperability (PI) Programs. To align with the renaming of the EHR Incentive Programs, we propose to remove references to the EHR Incentive Programs and replace them with ''Promoting Interoperability Programs'' in the 2015 Edition ''automated numerator recording'' criterion in § 170.315(g)(1) and the ''automated measure calculation'' criterion in § 170.315(g)(2).

V. Modifications to the ONC Health IT Certification Program

A. Corrections

1. Auditable Events and Tamper Resistance

Currently, § 170.315(d)(2), ''auditable events and tamper resistance,'' includes a cross- reference to § 170.315(d)(7). However, the cross reference to § 170.315(d)(7), ''end-user device encryption,'' does not always apply. We propose to revise § 170.550(h)(3) to apply the § 170.315(d)(7) cross reference as appropriate and exempt § 170.315(d)(7) when the certificate scope does not require § 170.315(d)(7) certification (*see* § 170.315(d)(2)(i)(C)). Paragraph 170.315(d)(2)(i)(C) is not applicable for the privacy and security testing and certification of a Health IT Module required by § 170.550(h)(3)(iii), (v), (vii), and (viii). This specific requirement was intended to be exempted. It would only apply if § 170.315(d)(7) was also required for privacy and security testing and certification, which it is not under the aforementioned paragraphs. For example, a developer that is seeking to certify a Health IT Module to § 170.315(h) will not necessarily have end-user device encryption features (*see* § 170.315(d)(7)). As such, certification can proceed for the audit log process without the Health IT Module demonstrating that it can record an encryption status as required by § 170.315(d)(2)(i)(C). We have previously identified this error in guidance and now propose to codify the correction in regulation.[39]

2. Amendments

We propose to revise § 170.550(h) to remove the ''amendments'' criterion's application to certain non-applicable clinical criteria including: ''Drug-drug, drug-allergy interaction checks for computerized provider order entry (CPOE)'' § 170.315(a)(4); ''clinical decision support'' § 170.315(a)(9); ''drug-formulary and preferred drug list checks'' § 170.315(a)(10); and ''patient-specific education'' § 170.315(a)(13). Health IT Modules presented for certification to these criteria would not have to demonstrate the capabilities required by the 2015 Edition ''amendments'' certification criterion (§ 170.315(d)(4)), unless the health IT is presented for certification to another criterion that requires certification to the 2015 Edition ''amendments'' criterion under the P&S certification framework. This has already been incorporated into sub- regulatory guidance, and we propose to codify this clarification in regulation.[40] The revision was made upon further analysis of the P&S certification framework and the applicability of the ''amendments'' certification criterion § 170.315(d)(4) to health IT capabilities that would not necessarily have any patient data for which a request for an amendment would be relevant.

3. View, Download, and Transmit to 3rd Party

We propose to remove § 170.315(e)(1)(ii)(B) which includes a cross-reference to § 170.315(d)(2). This cross-reference indicates that health IT may demonstrate compliance with activity history log requirements if it is also certified to the 2015 Edition ''auditable events and tamper-resistance'' certification criterion (§ 170.315(d)(2)). However, we no longer require testing of activity history log when certifying for § 170.315(d)(2). Therefore, this cross-reference is no longer applicable to meet certification requirements for the 2015 Edition ''view, download, and transmit to 3rd party'' certification criterion (§ 170.315(e)(1)) activity history log requirements.

4. Integrating Revised and New Certification Criteria Into the 2015 Edition Privacy and Security Certification Framework

Consistent with the 2015 Edition privacy and security certification framework, each certification criterion has a set of appropriate P&S ''safeguards'' that must be in place. In the 2015 Edition, we required that an ONC–ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text ''first level paragraph'' category of § 170.315 (*e.g.,* § 170.315(a)) identified below would be certified to either Approach 1 (technically demonstrate) or Approach 2 (system documentation). In this proposed rule, we propose to require the new criteria (§ 170.315(d)(12) and (d)(13)) to apply to all § 170.315 certification criteria. Therefore, given these and the other modifications discussed above, we propose to revise the P&S certification framework as

[39] *https://www.healthit.gov/sites/default/files/2015Ed_CCG_d2-Auditable-events-tamper-resistance.pdf.*

[40] *https://www.healthit.gov/sites/default/files/2015Ed_CCG_a4-DD-DAI-checks-for-CPOE.pdf, https://www.healthit.gov/sites/default/files/2015ed_ccg_a9-clinical-decision-support.pdf, https://www.healthit.gov/sites/default/files/2015Ed_CCG_a10-Drug-formulary-PDL-checks.pdf,* and *https://www.healthit.gov/sites/default/files/2015Ed_CCG_a13-Patient-specific-ed-resources.pdf.*

noted in the table below. However, the P&S Certification Framework would need to be further updated depending on finalization of the proposals discussed in section III.B.4, which propose removal of certain 2015 Edition certification criteria.

TABLE 1—PROPOSED 2015 EDITION PRIVACY AND SECURITY CERTIFICATION FRAMEWORK

If the Health IT Module includes capabilities for certification listed under:	It will need to be certified to approach 1 or approach 2 for each of the P&S certification criteria listed in the "approach 1" column	
	Approach 1	Approach 2
§ 170.315(a)(1), through (2), (5), through (8), (11), and (12).	§ 170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6) (emergency access), and (d)(7) (end-user device encryption).	For each applicable P&S certification criterion not certified using Approach 1, the health IT developer submits system documentation that is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable P&S certification criterion that enable the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion.
§ 170.315(a)(4), (9), (10), and (13).	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(7).	
§ 170.315(b)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) (integrity).	
§ 170.315(c)	§ 170.315(d)(1) through (d)(3) and (d)(5) *.	
§ 170.315(e)(1)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(7), and (d)(9)(trusted connection).	
§ 170.315(e)(2) and (3)	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(9) *.	
§ 170.315(f)	§ 170.315(d)(1) through (d)(3) and (d)(7).	
§ 170.315(g)(7) through (g)(11).	§ 170.315(d)(1) and (d)(9); and (d)(2) or (d)(10) (auditing actions on health information).	
§ 170.315(h)	§ 170.315(d)(1) through (d)(3) *.	
§ 170.315(b)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) (integrity).	
§ 170.315(c)	§ 170.315(d)(1) through (d)(3) and (d)(5).	
§ 170.315(e)(1)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(7), and (d)(9)(trusted connection).	
§ 170.315(e)(2) and (3)	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(9).	

§ 170.315(a)–(h) Certification Criterion

§ 170.315(a) through (h) Certification Criterion	§ 170.315(d)(12)
§ 170.315(a) through (h) Certification Criterion	§ 170.315(d)(13)

An ONC–ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text "first level paragraph" category of § 170.315 (e.g. § 170.315(a)) identified in the table above is certified to either Approach 1 (technically demonstrate) or Approach 2 (systemdocumentation). In addition, we propose that health IT developers seeking certification to any § 170.315 certification criterion for their Health IT Modules attest to whether they encrypt authentication credentials (§ 170.315(d)(12)) and support multifactor authentication (§ 170.315(d)(13))

We clarify that of the adopted 2015 Edition certification criteria, only the privacy and security criteria specified in § 170.315(g)(1) through (6) are exempt from the 2015 Edition privacy and security certification framework due to the capabilities included in these criteria, which do not implicate privacy and security concerns.

In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion identified as part of Approach 1 or Approach 2 so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the certification of a Health IT Module to § 170.315(e)(1) "view, download, and transmit to 3rd party" and (e)(2) "secure messaging." For each of these criteria, a Health IT Module must be separately tested to § 170.315(d)(9) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each criterion, respectively. We also propose the health IT developers seeking certification to any § 170.315 certification criterion for their Health IT Modules attest to whether they encrypt authentication credentials (§ 170.315(d)(12)) and support multi-factor authentication (§ 170.315(d)(13))

* § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

B. Principles of Proper Conduct for ONC–ACBs

1. Records Retention

We propose to revise the records retention requirement in § 170.523(g) to include the ''life of the edition'' as well as 3 years after the retirement of an edition related to the certification of Complete EHRs and Health IT Module(s). In the 2015 Edition final rule (80 FR 62602), we adopted a records retention provision that required ONC–ACBs to retain all records related to the certification of Complete EHRs and Health IT Module(s) for the ''life of the edition'' plus an additional 3 years, and the records would be available to HHS upon request during this period of time. In the 2015 Edition final rule, the ''life of the edition'' was defined as beginning with the codification of an edition of certification criteria in regulation and ending when the edition is removed from regulation. We now propose to clarify that HHS has the ability to access certification records for the ''life of the edition,'' which begins with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations, not solely during the 3-year period after removal from the CFR.

2. Conformance Methods for Certification Criteria

The Principle of Proper Conduct (PoPC) in § 170.523(h) specifies that ONC–ACBs may only certify health IT that has been tested by ONC–ATLs using tools and test procedures approved by the National Coordinator. We propose to revise this PoPC in three ways. First, we propose to revise this PoPC to additionally permit ONC–ACBs to certify Health IT Modules that they have evaluated for conformance with certification criteria without first passing through an ONC–ATL. However, we propose that such methods to determine conformity must first be approved by the National Coordinator. This proposal provides valuable Program flexibility and market efficiencies for streamlining Health IT Module certification, acknowledging the broad spectrum of evidence of conformance, from laboratory testing with an ONC–ATL to developer self-declaration. This Program flexibility will also allow us to leverage the success we have seen in implementation of our alternative test method process where any entity can submit a test procedure and/or test tool for approval for use under the Program. For example, the National Coordinator may, under this provision, approve a conformance method for certification criteria where evidence of a valid declaration of conformity (*e.g.,* certification) granted under an external program can be submitted directly to an ONC–ACB to meet the requirement of that certification criteria.

Second, we propose to revise the PoPC to clarify that certifications can only be issued to Health IT Modules and not Complete EHRs. We are proposing to remove the 2014 Edition from the CFR (*see* section II.B.2 of this preamble) and Complete EHR certifications are no longer available for certification to the 2015 Edition (80 FR 62608; 79 FR 54443). We propose to remove the provision that permits the use of test results from National Voluntary Laboratory Accreditation Program (NVLAP)-accredited testing laboratories under the Program because the regulatory transition period from NVLAP-accredited testing laboratories to ONC–ATLs has expired (81 FR 72447).

Third, we propose to remove the provision that permits the certification of health IT previously certified to an edition if the certification criterion or criteria to which the Health IT Module(s) was previously certified have not been revised and no new certification criteria are applicable because the circumstances that this provision seeks to address are no longer feasible with certification to the 2015 Edition. Any Health IT Module previously certified to the 2014 Edition and presented for certification to the 2015 Edition would have at least one new or revised 2015 Edition certification criteria that would be applicable. For example, the 2015 Edition ''accessibility-centered design'' criterion (§ 170.315(g)(5)) is applicable to any Health IT Module presented for certification to the 2015 Edition.

3. ONC–ACBs To Accept Test Results From Any ONC–ATL in Good Standing

We propose to revise the PoPC for ONC–ACBs in order to address business relationships between ONC–ACBs and ONC–ATLs. To encourage market competition, we propose to require ONC–ACBs to accept test results from any ONC–ATL that is in good standing under the Program and is compliant with its ISO 17025 accreditation requirements. However, if an ONC–ACB has concerns about accepting test results from a certain ONC–ATL, the ONC–ACB would have an opportunity to explain the potential issues to ONC and NVLAP, and on a case-by-case basis, ONC could consider the facts and make the final determination.

ONC–ATLs must be accredited by the NVLAP and seek authorization from ONC to participate in the ONC Health IT Certification Program. ONC–ATLs test products against the ONC-approved test method for the standards and certification criteria identified by the Secretary using ONC-approved test methods. ONC–ACBs make certification determinations and conduct surveillance for health IT originally tested by an ONC–ATL. Based on the process that all ONC-ATLs must undergo, we believe that they are capable of providing accurate test results that should be accepted by any ONC–ACB.

The intent of this proposal is to ensure that ONC–ATLs are not discriminated against and do not suffer injury from ONC–ACBs not accepting their test results if, in fact, they are in good standing. This proposal may also prevent harm to health IT developers, who present their health IT to be tested by ONC–ATLs and ultimately seek certification by ONC–ACBs under the Program. These situations may arise if a health IT developer's ONC–ACB leaves the Program or goes out of business. This proposal may also prevent situations of preferential business arrangements such as when one organization is both an ONC–ATL and ONC–ACB and will not enter into a contract with another organization who is also an ONC–ATL.

4. Mandatory Disclosures and Certifications

We propose to revise the PoPC in § 170.523(k). We propose to remove § 170.523(k) (1)(ii)(B) because certifications can only be issued to Health IT Modules and not Complete EHRs. We are proposing to remove the 2014 Edition from the CFR (*see* section III.B.2 of this preamble) and Complete EHR certifications are no longer available for certification to the 2015 Edition (80 FR 62608; 79 FR 54443). We also propose to revise § 170.523(k)(1)(iii) to broaden the section beyond just the Medicare and Medicaid EHR Incentive Programs (now referred to as Promoting Interoperability Programs). We propose to revise the section to include a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities, whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification.

We also propose to remove the provision in § 170.523(k)(3) that requires a certification issued to a pre-coordinated, integrated bundle of Health IT Modules to be treated the same as a certification issued to a Complete EHR for the purposes of § 170.523(k)(1), except that the certification must also indicate each Health IT Module that is included in the bundle. We propose to remove this provision because pre-coordinated, integrated bundles are no longer applicable for certification under Program.

We propose to revise § 170.523(k)(4) to clarify that a certification issued to a Health IT Module based solely on the applicable certification criteria adopted by the ONC Health IT Certification Program must be separate and distinct from any other certification(s) based on other criteria or requirements. The intent of this provision, as indicated in the Establishment of the Permanent Certification Program for Health Information Technology final rule (76 FR 1272), is to ensure that any other certifications an ONC–ACB may issue, is separately indicated from the applicable certification criteria adopted by the ONC Health IT Certification Program.

We also propose changes related to transparency attestations and limitations in section III.B.5. of this preamble. Additionally, we propose other new PoPCs for ONC–ACBs in sections VII.B.5 and VII.D of this preamble.

C. Principles of Proper Conduct for ONC–ATLs—Records Retention

We propose to revise the records retention requirement in § 170.524(f) to include the ''life of the edition'' as well as 3 years after the retirement of an edition related to the certification of Health IT Module(s). The circumstances are the same as in section V.B.1 of this preamble mentioned above, therefore, we propose the same revisions for ONC–ATLs as we did for ONC-ACBs.

VI. Health IT for the Care Continuum

ONC believes health IT should help promote and support patient care when and where it is needed. This means health IT should help support patient populations, specialized care, transitions of care, and practice settings across the care continuum. In the Permanent Certification Program final rule, we clarified that section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a voluntary certification program or programs for other types of health IT beyond those which supported the EHR Incentive Programs (now called the Promoting Interoperability Programs). However, we decided that the initial focus of the Program should be on supporting the EHR Incentive Programs, which focuses on EHR technology for the ambulatory and inpatient settings (76 FR 1294). As the Program evolved and the adoption and use of certified health IT increased significantly, we modified the Program in the 2015 Edition final rule to make it more open and accessible to more types of health IT, including health IT that supports various care and practice settings beyond those included in the EHR Incentive Programs (80 FR 62604). Our goal was then and is now to support the advancement of interoperable health IT and to promote health IT functionality in care and practice settings across the care continuum (*see also* 80 FR 62604).

ONC's efforts in the 2015 Edition to make the Program more open and accessible to other care settings also aligned with fall 2013 recommendations from the HIT Policy Committee (HITPC). The HITPC examined the extension of the Program to include functionalities that would benefit settings not covered by the EHR Incentive Programs. The HITPC recommended that considerations regarding functionality should focus on whether the functionality would:

- Advance a national priority or legislative mandate
- Align with existing federal/state programs
- Utilize the existing technology pipeline
- Build on existing stakeholder support
- Appropriately balance the costs and benefits of a certification program.

Taking into consideration the HITPC recommendations, ONC's 2015 Edition focused on the adoption of certification criteria that are standards-based, applicable to a wide variety of care and practice settings, and that advance the structured recording, access, exchange, and use of health information. ONC has also encouraged users—including specialty groups—to continue to work with developers to innovate, develop, and deploy health IT in specific clinical settings in ways that promote safety, effectiveness, and efficient health care delivery while also reducing burden.

In the 2015 Edition final rule we stated that we did not intend to develop and issue separate regulatory certification ''paths'' or ''tracks'' for particular care or practice settings (*e.g.,* a ''long-term and post-acute care (LTPAC) certification'') because it would be difficult to *independently* construct such ''paths'' or ''tracks'' in a manner that would align with other relevant programs and specific stakeholder needs. While we never have had intentions to adopt care- or practice-specific certification tracks, or additional voluntary program(s), in parallel to the existing voluntary ONC Health IT Certification Program, we stated that we would welcome the opportunity to work with HHS agencies, other agencies, and provider associations in identifying the appropriate functionality and certification criteria in the Program to support their stakeholders (80 FR 62704). This approach is consistent with the recommendations by the HITPC.

Since the publication of the 2015 Edition final rule, ONC has explored how we might work with the industry and with specialty organizations to collaboratively advance health IT that supports medical specialties and sites of service. As a result, we have gained insight from stakeholders regarding the burdens associated with establishing a specific set of required certification criteria for all users—which may include capabilities not applicable to certain settings of care or specialties. Stakeholders have also noted that the adoption of a set of required criteria without also enabling and incentivizing innovation beyond those criteria may have the unintended consequence of stifling progress for that setting. Stakeholders noted that the timeline for testing and certifying to required criteria and the subsequent deployment of certification criteria in practice settings is not always aligned with standards updates, the emergence of new standards, or technological innovation. Finally, stakeholders have urged ONC to leverage multiple means to advance interoperability standards that are widely applicable, to enable and promote innovation that is supported by these standards, and—in collaboration with stakeholders to monitor and support developments in emerging standards and technologies for specialty use cases.

Section 4001(b)(i) of the Cures Act instructs the National Coordinator to encourage, keep, or recognize, through existing authorities, the voluntary certification of health IT under the Program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. This provision of the Cures Act closely aligns with ONC's ongoing collaborative efforts with both federal partners and stakeholders within the health care and health IT community to encourage and support the advancement of health IT for a wide range of clinical settings. These initiatives have included projects related to clinical priorities beyond those specifically included in the EHR Incentive Programs (now called the Promoting Interoperability Programs) including efforts in public health, behavioral health, and long-term and post-acute care. We further note that these initiatives often include the development of non-regulatory informational resources to support the specific implementation goal and align with the technical specifications already available in the Program for certification. To advance these efforts, we generally consider a range of factors including: stakeholder input and identification of clinical needs and clinical priorities, the evolution and adoption of health IT across the care continuum, the costs and benefits associated with any policy or implementation strategy related to care settings and sites of service, and potential regulatory burden and compliance timelines. Generally, ONC's approach can be summarized in three parts:

- First, ONC analyzes existing certification criteria to identify how such criteria may be applicable for medical specialties and sites of service.
- Second, ONC focuses on the real-time evaluation of existing and emerging standards to determine applicability to medical specialties and sites of service as well as to the broader care continuum, including the evaluation of such standards for inclusion in the ONC Interoperability Standards Advisory (ISA).[41]
- Third, ONC may work in collaboration with stakeholders to support the development of informational resources for medical specialties and sites of service for which ONC identifies a need to advance the effective implementation of certified health IT.

We believe this approach provides an economical, flexible, and responsive option for both health care providers and the health IT industry, which is also in alignment with the provisions of the Cures Act related to burden reduction and promoting interoperability. We are committed to continuing to work with stakeholders in this manner to encourage and advance the adoption of health IT to support medical specialties and sites of service, and to help ensure that providers have the tools they need to support patients at the point of care and that essential patient health information is available across a care settings.

This section outlines our approach to implement Section 4001(b) of the Cures Act, which requires that the Secretary make recommendations for the voluntary certification of health IT for use by pediatric health providers and to adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children. To be clear, and consistent with past practice, we do not recommend or propose a ''pediatric-specific track or program'' under the ONC Health IT Certification Program. This proposed rule outlines the certification criteria adopted in the 2015 Edition which we believe support the certification of health IT for pediatric care. Finally, it identifies the new and revised criteria proposed in this rule which we believe further support the voluntary certification of health IT for pediatric care. We have included in the appendix of this proposed rule a set of technical worksheets that can help inform your comments on the recommendations, the new and revised criteria in the Program that would also support pediatric care settings, and the overall approach we have herein described. These worksheets outline the following information:

- The alignment of each recommendation to the Children's Model EHR Format[42] as identified by stakeholders (see also Section VI.A.1 and 2 for further detail on the Children's Model EHR Format and the recommendations).
- The alignment of each recommendation to the 2015 Edition certification criteria and new or revised criteria described in this proposed rule (see also section VI.A.2.a and b).
- Potential supplemental items from the Children's Model EHR Format identified by ONC which relate to the primary recommendation and the related certification criteria.

We invite readers to use these worksheets to inform public comment on the recommendations and criteria described in Section VI.A.2 specifically as they relate to pediatric health care use cases. The comments received on these technical worksheets through this proposed rule will be used to inform the final recommendations for voluntary certification of health IT criteria for use in pediatric care. Furthermore, these comments, and the detailed insights received through stakeholder outreach, may inform the future development of a non-binding informational guide or resource to provide useful information for health IT developers and pediatric care providers seeking to successfully implement these health IT solutions in a clinical setting.

A. Health IT for Pediatric Setting

Section 4001(b)(iii) of the Cures Act—''Health information technology for pediatrics'' requires that:

- First, that the Secretary, in consultation with relevant stakeholders, shall make recommendations for the voluntary certification of health IT for use by pediatric health providers to support the health care of children, and
- Second, that the Secretary shall adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children.

In this proposed rule, we describe our approach to stakeholder engagement, the analysis used to develop the recommendations, and the specific certification criteria we believe can support each recommendation.

1. Background and Stakeholder Convening

Over the past ten years, a number of initiatives have focused on the availability and use of effective health IT tools and resources for pediatric care. These have included a number of public-private partnerships including efforts between HHS, state agencies, and health systems for innovative projects that range from care coordination enterprise solutions to immunization information systems and to point of care solutions for specialty needs. In order to learn from and build upon these efforts, ONC has engaged with stakeholders in both the public and private sector including other federal, state and local government partners, health care providers engaged in the care of children, standards development organizations, charitable foundations engaged in children's health care research, and health IT developers supporting pediatric care settings.

For example, significant work has been done by the Agency for Healthcare Research and Quality (AHRQ), CMS, the Health Resources and Services Administration (HRSA), and organizations around the Children's Model EHR Format (Children's Format), which is critical to any discussion of the pediatric health IT landscape.[43] The Children's Format was authorized by the 2009 Children's Health Insurance Program Reauthorization Act (CHIPRA)[44] and developed by AHRQ in

[41] *https://www.healthit.gov/isa/.*

[42] *https://healthit.ahrq.gov/health-it-tools-and-resources/pediatric-resources/childrens-electronic-health-record-ehr-format.*

[43] Agency for Health Care Information and Technology. Health Information Technology. *http://healthit.ahrq.gov/health-it-tools-and-resources/childrens-electronic-health-record-ehr-format* Accessed September, 2017.

[44] Public Law 111–3, section 401.

close collaboration with CMS. It was developed to bridge the gap between the functionality present in most EHRs currently available and the functionality that could optimally support the care of children. Specifically, the Children's Format provides information to EHR system developers and others about critical functionality and other requirements that are helpful to include in an EHR system to address health care needs specific to the care of children. The final version of the Children's Format,[45] released in 2015, consists of 47 high priority functional requirements in 19 topic areas that focus on improvements that would better support the safety and quality of care delivered to children. The Children's Format was intended as a starting point for developers, users, and purchasers for informing an approach for pediatric voluntary certification. We refer to the Voluntary Edition proposed rule for a description of ONC's prior discussion around the Children's Format (79 FR 10930).

In the summer of 2017, the American Academy of Pediatrics (AAP) reviewed the 2015 Format using a robust analytical process and engagement with their members. The result was a prioritized list of eight clinical priorities to support pediatric health care (''Priority List''). In October 2017, ONC held a technical discussion with stakeholders titled ''Health IT for Pediatrics'' with the specific purpose of obtaining input from an array of stakeholders in an effort to draw correlations between the pediatric providers' clinical priorities identified in the Priority List with the detailed technical requirements outlined in the Children's Format and the capabilities and standards that could be included in certified health IT. Through this collaborative approach, the meeting participants identified a set of priority needs for health IT to support pediatric care based upon those identified by the Priority List and the primary correlation to the Children's Format.

2. Recommendations for the Voluntary Certification of Health IT for Use in Pediatric Care

To support the first part of Section 4001(b) of the Cures Act, ONC considered the historical efforts on the Children's Model EHR Format, the input from stakeholders, and our own technical analysis and review of health IT capabilities and standards to develop a set of recommendations for voluntary certification for health IT for pediatric care. These include eight recommendations related to the Priority List:

- *Recommendation 1:* Use biometric-specific norms for growth curves and support growth charts for children.
- *Recommendation 2:* Compute weight-based drug dosage.
- *Recommendation 3:* Ability to document all guardians and caregivers.
- *Recommendation 4:* Segmented access to information.
- *Recommendation 5:* Synchronize immunization histories with registries.
- *Recommendation 6:* Age- and weight-specific single-dose range checking.
- *Recommendation 7:* Transferrable access authority.
- *Recommendation 8:* Associate maternal health information and demographics with newborn.

We also developed two additional recommendations beyond the Priority List which relate to other items within the Children's Format that are considered important to pediatric stakeholders. These additional recommendations, which we believe may be supported by certified health IT, are as follows:

- *Recommendation 9:* Track incomplete preventative care opportunities.
- *Recommendation 10:* Flag special health care needs.

In order to implement the second part of Section 4001(b) of the Cures Act for the adoption of certification criteria to support the voluntary certification of health IT for use by pediatric health care providers, we have identified both the 2015 Edition certification criteria and the new or revised criteria in this proposed rule that we believe support these 10 recommendations for health IT for pediatric care and sites of service. We direct readers to the appendix of this proposed rule for a set of technical worksheets which include a cross-walk of the various criteria specifically associated with each recommendation. These worksheets outline the following information:

- The alignment of each recommendation to the primary Children's Format[46] item identified by stakeholders.
- The alignment of each recommendation to the 2015 Edition certification criteria and new or revised criteria described in this proposed rule.
- Supplemental items from the Children's Format for each recommendation and the related certification criteria.

We invite readers to use these worksheets to inform public comment on the recommendations, the inclusion of specific items from the Children's Format, and the identified certification criteria as they relate specifically to use cases for pediatric care and sites of service. We also seek comment on the following:

1. Relevant gaps, barriers, safety concerns, and resources (including available best practices, activities, and tools) that may impact or support feasibility of the recommendation in practice.
2. Effective use of health IT itself in support of each recommendation as involves provider training, establishing workflow, and other related safety and usability considerations.
3. If any of the 10 recommendations should not be included in ONC's final recommendations for voluntary certification of health IT for pediatric care.
4. Any certification criteria from the Program that is identified for the 10 recommendations that should not be included to support the specific recommendation.

As stated in the worksheets located in the appendix, commenters are encouraged to reference the specific ''recommendation number'' (1–10) with the corresponding technical worksheet question number in their response. For example, ''Recommendation 1—Question 3''.

a. 2015 Edition Certification Criteria

In order to implement the second part of Section 4001(b) of the Cures Act to adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children, we identified the following 2015 Edition certification criteria that support the recommendations. Within the technical worksheets in the appendix of this proposed rule, these criteria are noted under each recommendation to which they are correlated. The 2015 Edition criteria are as follows:

- ''API functionality'' criteria (§ 170.315(g)(7)–(g)(9)) which addresses many of the challenges currently faced by patients and by caregivers such as parents or guardians accessing child's health information, including the ''multiple portal'' problem, by potentially allowing individuals to aggregate health information from multiple sources in a web or mobile application of their choice.
- ''Care plan'' criterion (§ 170.315(b)(9)) which supports

[45] *https://healthit.ahrq.gov/sites/default/files/docs/citation/children-ehr-format-enhancement-final-recommendation-report-abridged.pdf.*

[46] *https://healthit.ahrq.gov/health-it-tools-and-resources/pediatric-resources/childrens-electronic-health-record-ehr-format.*

pediatric care by facilitating the documentation of electronic health information in a structured format to improve care coordination (80 FR 62648–62649).

- ''Clinical decision support'' (CDS) criterion (§ 170.315(a)(9)) which supports pediatric care by enabling interventions based on the capture of biometric data.
- ''Common Clinical Data Set'' (adopted in (§ 170.315(b)(4) and § 170.315(b)(5)) which includes *optional* pediatric vital sign data elements including as optional the reference range/growth curve for three pediatric vital signs—BMI percent per LOINC identifiers for age per sex, weight per length/sex, and head occipital-frontal circumference for children less than three years of age.
- ''Data segmentation for privacy'' send criterion and receive criterion (adopted in § 170.315(b)(7) and § 170.315(b)(8)) which provides the ability to: Create a summary record that is tagged at the document level as restricted and subject to re-disclosure; receive a summary record that is document-level tagged as restricted; separate the document-level tagged document from other documents received; and, view the restricted document without having to incorporate any of the data from the document.
- ''Demographics'' criterion (§ 170.315(a)(5)) which supports pediatric care through the capture of values and value sets relevant for the pediatric health care setting as well as allowing for improved patient matching which is a key challenge for pediatric care.
- ''Electronic Prescribing'' criterion (adopted in § 170.315(b)(3)) which includes an *optional* Structured and Codified Sig Format, which has the capability to exchange weight-based dosing calculations within the NCPDP SCRIPT 10.6 standard and limits the ability to prescribe all oral, liquid medications in only metric standard units of mL (*i.e.,* not cc) important for enabling safe prescribing practices for children.
- ''Family health history'' criterion (§ 170.315(a)(12)) which supports pediatric care because it leverages concepts or expressions for familial conditions, which are especially clinically relevant when caring for children.
- ''Patient health information capture'' criterion (§ 170.315(e)(3)) which supports providers' ability to accept health information from a patient or authorized representative. This criterion could support pediatric care through documentation of decision-making authority of a patient representative.
- ''Social, psychological, and behavioral data'' criterion § 170.315(a)(15) which supports integration of behavioral health data into a child's record across the care continuum by enabling a user to record, change, and access a patient's social, psychological, and behavioral data based using SNOMED CT® and LOINC® codes.
- ''Transitions of care'' criterion (§ 170.315(b)(1)) which supports structured transition of care summaries and referral summaries that help ensure the coordination and continuity of health care as children transfer between different clinicians at different health care organizations or different levels of care within the same health care organization;
- ''Transmission to immunization registries'' criterion (§ 170.315(f)(1)) which supports the safe and effective provision of child health care through immunizations and registry linkages. This criterion also provides the ability to request, access, and display the evaluated immunization history and forecast from an immunization registry for a patient. Immunization forecasting recommendations allow for providers to access the most complete and up-to-date information on a patient's immunization history to inform discussions about what vaccines a patient may need based on nationally recommended immunization recommendations (80 FR 62662–62664).
- ''View, download, and transmit to 3rd party'' (VDT) criterion (§ 170.315(e)(1)) which supports transferrable access authority for the pediatric health care setting and provides the ability for patients (and their authorized representatives) [47] to view, download, and transmit their health information to a 3rd party.

We note that some of these criteria may be updated based on proposals contained in this proposed rule; however, we believe that prior to any such updates, technology that is currently available and certified to these 2015 Edition criteria can make a significant impact in supporting providers engaged in the health care of children. We invite readers to use the technical worksheets in the appendix to this proposed rule to inform their public comment on the recommendations, the inclusion of specific items from the Children's Format, and the identified 2015 Edition certification criteria as they relate specifically to use cases for pediatric care and sites of service.

b. New or Revised Certification Criteria in This Proposed Rule

In order to implement the second part of Section 4001(b)(iii) of the Cures Act to adopt certification criteria to support the voluntary certification of health information technology for use by pediatric health providers to support the health care of children, we identified new or revised certification criteria in this proposed rule that support the recommendations. These new or revised criteria and standards in this proposed rule that would support pediatric settings include:

- New API criterion (§ 170.315(g)(10)) which would serve to implement the Cures Act requirement to permit health information to be accessed, exchanged, and used from APIs without special effort (see section IV.B.5 of this proposed rule).
- New ''DS4P'' criteria (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) that would support a more granular approach to privacy tagging data for health information exchange supported by either the C–CDA- or FHIR-based exchange standards (see section VI.A for a discussion of this criteria in relation to pediatric settings and section VI.B for discussion of these criteria in relation to Opioid Use Disorder).
- New electronic prescribing certification criterion (§ 170.315(b)(11)), which would supports improved patient safety and prescription accuracy, workflow efficiencies, and increased configurability of systems including functionality that could support pediatric medication management.
- USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference (and the criteria that include the USCDI).

Each of these proposed criteria are further described in other sections of this proposed rule; however, in this section of this proposed rule we specifically seek comment on the application of these criteria to pediatric use cases in support of our recommendations for the voluntary certification of health IT for pediatric care.

[47] The VDT criterion includes a ''patient-authorized representative'' concept that aligns with the use of the term under the EHR Incentive Program. A ''patient-authorized representative'' is defined as any individual to whom the patient has granted access to their health information (see also 77 FR 13720). However, consent is not needed for minors, for whom existing local, state, or federal law grants their parents or guardians access (see also 77 FR 13720).

For example, our proposal for three new 2015 Edition DS4P certification criteria (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) could provide functionality to address the concerns of multiple stakeholders in a range of specialty use cases—including pediatric care settings. In this section of this proposed rule, we seek comment specifically related to the inclusion of these criteria in our recommendations. Specifically, stakeholders have expressed the need to—based on the intended recipient of the data—to restrict granular pediatric health data at production. We believe these criteria could, for example, help enable providers to:

- Limit the sharing of reproductive and sexual health data from an EHR in order to protect the minor's privacy;
- Prevent disclosure of an emancipated minor's sensitive health information, while also permitting a parent or legal guardian to provide consent for treatment; and
- Segment child abuse information based on jurisdictional laws, which may have varying information sharing requirements for parents, guardians, and/or other possible legal representatives.

While health care providers should already have processes and workflows in place to address their existing compliance obligations, we recognize that more granular privacy markings at the point of data capture would further support existing and future priorities of pediatric health providers, as well as for multiple medical specialties and sites of service. We also recognize that such point of data capture markings can reduce administrative burden through efficiencies gained in streamlined compliance workflows.

We invite readers to use the technical worksheets in the appendix of this proposed rule to support public comment on the recommendations, the inclusion of specific items from the Children's Format, and the identified proposed new or revised certification criteria as they relate specifically to use cases for pediatric care and sites of service.

However, as discussed, through our experience and engagement with health care providers and health IT developers, we believe that in some cases information resources can aid in implementation in clinical settings. In the past, ONC has worked collaboratively with federal partners, health IT developers, and the health care community to support the development of non-regulatory informational resources that can provide additional support for health IT implementation (see, for example, the ONC Patient Engagement Playbook). Such a resource could include the recommendations and certification criteria here identified and synthesize these technical recommendations with information outside of the Program related to patient safety, usability, privacy and security, and other key considerations for successful implementation of a health IT system within a clinical setting. We believe that the creation of such a resource, in collaboration with clinical and technical stakeholders, would help support the advancement of health IT solutions for use in pediatric care and pediatric settings. We further include additional information on prior ONC initiatives related to health IT for pediatric settings as available on our website at *www.healthit.gov/pediatrics.*

B. Health IT and Opioid Use Disorder Prevention and Treatment—Request for Information

We have identified a need to explore ways to advance health IT across the care continuum to support efforts to fight the opioid epidemic. To that purpose, we seek comment in this proposed rule on a series of questions related to health IT functionalities and standards to support the effective prevention and treatment of opioid use disorder (OUD) across patient populations and care settings.

We recognize the significance of the opioid epidemic confronting our nation and the importance of helping to support health care providers committed to preventing inappropriate access to prescription opioids and providing safe, appropriate treatment.

HHS has a comprehensive strategy to combat the opioid crisis. It consists of five points that are focused on better: Addiction prevention, treatment, and recovery services; data; pain management; targeting of overdose reversing drugs; and research.[48] In support of this strategy, HHS will improve access to prevention, treatment, and recovery support services; target the availability and distribution of overdose-reversing drugs; strengthen public health data reporting and collection; support cutting-edge research; and advance the practice of pain management. To combat the opioid crisis, in October 2018, Congress passed the Substance Use-Disorder Prevention that Promotes Opioid Recovery and Treatment (SUPPORT) for Patients and Communities Act. It aims to expand treatment, recovery, and prevention initiatives for substance use disorder and also includes interoperability and health IT tools as a key part of the response to this crisis.

We believe health IT offers promising strategies to help medical specialties and sites of service as they combat opioid use disorder (OUD). For example, health IT has the potential to improve adherence to opioid prescribing guidelines and physician adherence to treatment protocols, to increase the safety of prescribing for controlled substances, to enhance clinician access to PDMPs, and to expand access to addiction treatment and recovery support services. Additionally, through the Program, our goal continues to be to improve access to data from disparate sources and help ensure that key data is consistently available to the right person, at the right place, and at the right time across the care continuum. One component of advancing that goal is through technical standards for exchanging health information that form an essential foundation for interoperability.

ONC has heard from stakeholders including policymakers, implementers, health care providers and patient advocacy groups that additional information is needed to assist in planning for the effective use of health IT in OUD prevention and treatment. We additionally recognize stakeholders' interest in the new opioid measures (Query of PDMP measure and Verify Opioid Treatment Agreement measure) included in CMS's Promoting Interoperability Programs (formerly known as the Medicare and Medicaid EHR Incentive Programs). These two measures support HHS initiatives related to the treatment of opioid and substance use disorders by helping health care providers avoid inappropriate prescriptions, improve coordination of prescribing amongst health care providers, and focus on the advanced use of certified health IT in care coordination for OUD prevention and treatment (83 FR 41644).

In order to support these efforts, in this proposed rule we outline a brief overview of some key areas of health IT implementation that could support OUD prevention and treatment. These include consideration of current health IT certification criteria included in the 2015 Edition, revised or new certification criteria as outlined in this proposed rule, and current health IT initiatives underway in the health care industry or health IT industry which intersect with ONC policy goals. In this section of the proposed rule, we request public comment specifically from the perspective of how our existing Program

[48] *https://www.hhs.gov/opioids/.*

requirements and proposals in this rulemaking may support use cases related to OUD prevention and treatment and if there are additional areas that ONC should consider for effective implementation of health IT-enabled OUD prevention and treatment. We seek comment from this perspective on the identification of 2015 Edition certification criteria, the proposals for revised or new certification criteria, and the potential future consideration of emerging technologies described in various initiatives.

1. 2015 Edition Certification Criteria

We seek public comment on how the existing 2015 Edition certification criteria as well as proposals within this proposed rule for revised or new criteria support OUD prevention and treatment. Specifically, we seek comment on certification criteria previously adopted in the 2015 Edition that can support clinical priorities, advance interoperability for OUD (including care coordination and the effective use of health IT for the treatment and prevention of OUD). In this proposed rule, we summarize some of these 2015 Edition certification criteria identified and indicate how they support care coordination, the prevention of OUD and overdose, and the detection of opioid misuse, abuse, and diversion.

We have also below identified the proposals for revised or new 2015 Edition criteria within this proposed rule that we believe can support clinical priorities, advance interoperability for OUD (including care coordination and also the effective use of health IT for the treatment and prevention of OUD). We welcome input from stakeholders specifically on these criteria within the context of OUD prevention and treatment, as well as input on the identification of other criteria included either in the 2015 Edition and/or that are proposed in other parts of this rule that may be considered a clinical and interoperability priority for supporting OUD treatment and prevention.

We have identified several 2015 Edition certification criteria available now for certification in the Program which could support care coordination and the prevention and detection of opioid misuse, abuse, and diversion. They are:

- The ''transitions of care'' criterion (§ 170.315(b)(1)) supports structured transition of care summaries and referral summaries that help ensure the coordination and continuity of health care as patients transfer between different clinicians at different health care organizations or different levels of care within the same health care organization. This criteria supports the ability to transmit a summary care record to support an individual with OUD upon discharge from an inpatient setting or from a primary care provider to another setting for their care.
- The ''clinical information reconciliation and incorporation'' criterion (§ 170.315(b)(2)) allows clinicians to reconcile and incorporate patient health information sent from external sources to maintain a more accurate and up-to-date patient record. This process could help—for example—reduce opioid related errors regarding patients who use multiple pharmacies, have co-morbidity factors, and visit multiple clinicians.
- The ''electronic prescribing'' criterion (§ 170.315(b)(3)) provides a way to write and transmit prescription information electronically. This criterion facilitates appropriate opioid prescribing by simplifying the review of prescription information during follow-up visits or transitions to other clinicians, by allowing prescribers to communicate prescription-related messages to pharmacies electronically and by capturing and transmitting medication histories that are shared with PDMPs. In this proposed rule, we propose to update the existing electronic prescribing certification criterion as described in section IV.B.2 of this proposed rule.
- The ''patient health information capture'' (§ 170.315(e)(3)) allows clinicians to incorporate unstructured patient generated health data or data from a non-clinical setting into a patient record. The CMS Promoting Interoperability Programs for eligible hospitals includes a new optional measure which is focused on verifying the existence of a signed Opioid Treatment Agreement for certain patients when a controlled substance is prescribed and incorporating it into the record. In the Hospital Inpatient Prospective Payment Systems final rule, CMS recognized this certification criterion's potential to support this goal within a certified health IT system (83 FR 41654).
- The ''social, psychological, and behavioral data'' criterion (§ 170.315(a)(15)) can help to provide a more complete view of a patient's overall health status. This is important to help provide a ''whole-patient'' approach to the treatment of substance use disorders included as part of Medicated-Assisted Treatment (MAT) that involves the use of FDA-approved medications, in combination with counseling and behavioral therapies, to treat individuals recovering from OUD. This data can help to improve care coordination and lead to the identification of appropriate social supports and community resources.

We seek comment on how these criteria and what additional 2015 Edition certification criteria may be considered a clinical and interoperability priority for supporting OUD treatment and prevention. We also seek comment on the value of developing a potential future non-binding informational guide or resource to provide useful information for OUD providers and sites of service related to specific clinical priorities and use cases of focus.

2. Revised or New 2015 Edition Certification Criteria in This Proposed Rule

This proposed rule contains additional proposals to revise or add new criteria to the Program to better support care across the continuum. We believe these criteria and standards, highlighted below, can also support treatment and prevention of OUD. We seek comment specifically on the applicability of these criteria to the OUD use case. They are:

- *USCDI:* As detailed in section IV.B.1, we are proposing to adopt the USCDI as a standard (§ 170.213) which would establish a minimum set of data classes (including structured data fields) that are required to be interoperable nationwide, and is designed to be expanded in an iterative and predictable way over time. The USCDI Version 1 (USCDI v1) builds upon the 2015 Edition CCDS and includes a common set of data classes that can be supported by commonly used standards. It includes the 2015 Edition CCDS data elements, such as medications. It also includes two new data classes, titled ''clinical notes'' and ''provenance,'' which would help facilitate interoperable exchange and the trustworthiness of the data being exchanged. These enhancements to the comprehensiveness and reliability of the data being exchanged could help empower physicians in the prevention and detection of opioid misuse, abuse, and diversion.

In addition, because we propose to adopt the USCDI as a standard, health IT developers would be allowed to take advantage of the Maintenance of Certification requirements described in section VII.B.5 of this proposed rule. Therefore, the USCDI would have the potential to further benefit clinical priorities and interoperability for OUD, including safe and appropriate opioid prescribing, through the ability to voluntarily implement and use a new version of an adopted standard or implementation specification so long as certain conditions are met, including the new version being approved by the National Coordinator for use in certification through the Standards Version Advancement Process. We seek comment on how this proposal would further support the access, exchange, and use of additional and future data classes (including structured data fields) in more care and practice settings specifically as related to the prevention and treatment of OUD.

- *Standardized API:* We are proposing new API functionality through the adoption of a new API certification criterion (§ 170.315(g)(10)), which serves to implement the Cures Act requirement to permit health information to be accessed, exchanged, and used from APIs without special effort. This criterion would enable efficient exchange of health information using modern internet technologies and thus enable collaborative, patient-driven, integrated care for individuals recovering from OUD.
- *Data Segmentation for Privacy and Consent Management:* As discussed in section IV.B.7, we are also proposing to remove the current 2015 Edition DS4P—send (§ 170.315(b)(7)) and DS4P—receive (§ 170.315(b)(8)) certification criteria. We propose to replace these two criteria with three new 2015 Edition DS4P certification criteria (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) that would support a more granular approach to privacy tagging data for health information exchange supported by either the C–CDA- or FHIR-based exchange standards. We believe this proposal would offer functionality that is more valuable to providers and patients, especially given the complexities of the privacy law landscape for multiple care and specialty settings. We also believe this proposal could lead to more complete records, contribute to patient safety, and enhance care coordination. Additionally, we believe this proposal may support a more usable display of OUD information at the request of patients within an EHR and we invite input on best practices, including the processes and methods by which OUD information should be displayed.
- *Electronic Prescribing and PDMPs:* As discussed in section IV.B.2, we are proposing to remove the current 2015 Edition electronic prescribing certification criterion (§ 170.315(b)(3)) and replace this criterion with a new electronic prescribing certification criterion (§ 170.315(b)(11)) that would support improved patient safety and prescription accuracy, create workflow efficiencies, reduce testing requirements, and increase configurability of systems. This new proposed criterion includes the addition of Risk Evaluation and Mitigation Strategy (REMS) messages. We believe this proposal would help address challenges discussed in the CMS Hospital Inpatient Prospective Payment Systems final rule (83 FR 41651) and Medicare Physician Fee Schedule proposed rule (83 FR 35704) by strengthening clinical and administrative efficiency, helping move the industry forward by adopting more current standards for electronic prescribing, and harmonizing efforts across federal agencies in the prevention and treatment of OUD. In addition, the FDA has enacted an opioids medications REMS program for opioid analgesics[49] mandating prescriber and patient education to encourage proper patient screening and appropriate monitoring. Adoption of the new proposed criterion also supports the efficient and accurate exchange of medication history transactions between providers and pharmacies, and between pharmacies and state PDMPs.

3. Emerging Standards and Innovations

In addition to the certification criteria established in the 2015 Edition final rule and proposed in this rule, ONC is engaged in a number of health IT and standards initiatives exploring innovation and emerging standards to inform future health IT policy. In some cases, these efforts may not be mature enough or best suited for adoption in the Program; however, we seek comment on the potential consideration of these initiatives for future direction of ONC policy.

- *CDS Hooks:* Improving how opioids are prescribed through evidence-based guidelines can ensure patients have access to safer, more effective chronic pain treatment while reducing the risk of opioid misuse, abuse, or overdose from these drugs. In response to the critical need for consistent and current opioid prescribing guidelines, the Centers for Disease Control and Prevention (CDC) released the Guideline for Prescribing Opioids for Chronic Pain.[50] While progress has been made in training prescribers and fostering the adoption of the CDC guideline, the President's Opioid Commission[51] acknowledged that ''not all states have adopted the guideline, not all physicians are aware of them, and sound opioid prescribing guidelines are far from universally followed.'' Clinical decision support (CDS) Hooks is a health IT specification that has the potential to positively affect prescriber adoption of evidence-based prescribing guidelines by invoking patient-specific clinical support from within the clinician's EHR workflow. ONC is currently collaborating with CDC on a project to translate the CDC guideline into standardized, shareable, computable decision support artifacts using CDS Hooks. We recognize that CDS Hooks is still an emerging technology and seek input on the adoption of the CDS Hooks specification for opioid prescribing and OUD prevention and treatment. We also request public comment on other health IT solutions and effective approaches to improve opioid prescription practices and clinical decision support for OUD.
- *Care Plan FHIR Resource:* A shared care plan is a critical concept for managing an individual's health across a continuum that includes both clinical and non-clinical settings[52] and can help enable more informed and useful connections among all the stakeholders engaged in preventing or treating OUD. For those in recovery from OUD, the care plan can enable patients to access their care plan information and coordinate their care with approved community care providers which is critical and part of evidence-based recovery treatment services. In 2015, the ONC HITPC recommended that the National Coordinator accelerate the implementation of dynamic, shared, longitudinal care plans that incorporate information from both clinical and non-clinical services and empower individuals to manage their own health and care.[53] A consideration for HHS as part of this earlier recommendation included looking at the future standards development needed to transition from the static care plan documentation (document template in C–CDA R2.1) to a dynamic shared care plan that supports more robust care coordination.[54] We believe HL7 standards and standardized APIs can elevate care coordination and care management across the continuum,

[49] *https://www.fda.gov/Drugs/DrugSafety/InformationbyDrugClass/ucm163647.htm.*

[50] *Guideline for Prescribing Opioids for Chronic Pain: https://www.cdc.gov/mmwr/volumes/65/rr/rr6501e1.htm.*

[51] President's Opioid Commission: *https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Final_Report_Draft_11-1-2017.pdf.*

[52] *https://www.healthit.gov/hitac/events/policy-advanced-health-models-and-meaningful-use-workgroup-8.*

[53] *https://www.healthit.gov/sites/default/files/facas/HITPC_AHM_Hearing_Transmittal_08-11-2015_0.pdf.*

[54] *https://www.healthit.gov/hitac/events/policy-advanced-health-models-and-meaningful-use-workgroup-8.*

including for those providers without EHRs, whether for opioid use disorder related treatment, primary health, or other problems. Indeed, numerous efforts are underway within HL7 and other collaborations to standardize ''care plans'' and their content using FHIR and the C–CDA. From a technical perspective and in the context of the proposals focused on the USCDI standard, the ARCH standard, the new proposed API certification criterion at 170.315(g)(10), and the voluntary Standards Version Advancement Process Maintenance of Certification requirement described in section VII.B.5 of this proposed rule, we can see a future where a (g)(10)–certified API would be capable of supporting care plan data. We request public comment on the current maturity of existing and forthcoming technical specifications to support care plan/care plan data as well as specific information that could be prioritized within a future USCDI data class focused on care plans.

In addition to commenting on the criteria noted in this section, we also encourage stakeholders to participate in the ISA process.[55] The ISA represents the model by which ONC coordinates the identification, assessment, and public awareness of interoperability standards and implementation specifications. ONC encourages all stakeholders to implement and use the standards and implementation specifications identified in the ISA as applicable to the specific interoperability needs they seek to address and encourages pilot testing and other industry experience adopting standards and implementation specifications identified as ''emerging'' in the ISA. The web-based version of the ISA documents known limitations, preconditions, and dependencies, and provide suggestions for security best practices in the form of security patterns for referenced standards and implementation specifications when they are used to address a specific clinical health IT interoperability need.

Additionally, through the ISA process, stakeholders are encouraged to comment on the outlined standards and implementation specifications, as ONC updates the ISA regularly. ONC has developed and has plans to develop further ISA content to highlight standards and implementation specifications that support the prevention and treatment of OUD/substance use disorder (SUD). For example, the NCPDP SCRIPT standard allows a prescriber to request a patient's medication history from a state PDMP via the RxHistoryRequest and RxHistoryResponse. ONC is also working to enhance the ISA to make it easier for stakeholders to find standards and implementation specifications related to high-priority use cases, such as OUD/SUD. The ISA has a comment process that occurs each year [56] and we encourage stakeholders to participate in that process to comment on other standards and implementation specifications that currently exist in the ISA or that the industry and its stakeholders feel should be added to the ISA that support OUD/SUD prevention, treatment, monitoring, and care coordination.

4. Additional Comment Areas

We further seek comment on effective approaches for the successful dissemination and adoption of standards including the NCPDP SCRIPT 2017071 standard (see section IV.B.2) that can support the exchange of PDMP data for integration into EHRs and also enable further adoption and use of Electronic Prescribing of Controlled Substances (EPCS). Regarding integration of health IT with PDMPs and EPCS, we believe there are real and perceived challenges and opportunities that involve policy and technical components. As we explore these issues in collaboration with industry and stakeholders, we seek comment on the priority challenges and opportunities for these topics and on any technical and policy distinctions, as appropriate.

We also note that there are many federal initiatives separate from ONC proposed rulemaking and the Program that exist within HHS programs including, but not limited to, CMS Medicaid and Medicare programs. For example, Medicare now provides separate payment for psychiatric collaborative care model/behavioral health integration and chronic care management services (see 81 FR 80233, and 80247), and Medicaid issued guidance on leveraging technology to address the opioid crisis at enhanced funding matches [56] and also includes SUD health IT in standard terms and conditions as part of 1115 waiver requirements.

In addition, CMS sought comment for consideration through separate rulemaking in both the 2019 Physician Fee Schedule proposed rule (83 FR 35923) and Hospital Inpatient Prospective Payment Systems proposed rule (83 FR 20528) regarding whether they should adopt the NCPDP SCRIPT 2017071 standard to facilitate future reporting of the proposed Query of PDMP quality measure. As noted in the Hospital Inpatient Prospective Payment Systems final rule, a few commenters supported the use of NCPDP Script Standard Implementation Guide Version 2017071 medication history transactions for PDMP queries and response. Additionally, CMS encourages advances in standards and their use to deliver innovative, interoperable solutions that will seamlessly integrate PDMP query functionality into clinician-friendly, patient- centered CEHRT-enabled workflows that facilitate safer, more informed prescribing practices and improved patient outcomes (83 FR 41651).

We seek comment on how successful implementation of health IT that supports OUD can aid in the achievement of national and programmatic goals, especially where they may align with initiatives across HHS and with stakeholder and industry led efforts.

Finally, we seek comment on a topic that involves health IT for both pediatric care and OUD prevention and treatment—Neonatal Abstinence Syndrome (or NAS). In its September 2018 report, *Facing Addiction in America: The Surgeon General's Spotlight on Opioids,* the HHS Office of the Surgeon General describes how the incidence of Neonatal Abstinence Syndrome (or NAS), has increased dramatically in the last decade along with increased opioid misuse. Newborns may experience NAS, a withdrawal syndrome, following exposure to drugs while in the mother's womb. NAS is an expected and treatable condition following repeated maternal substance use and abuse during pregnancy, which may have long-term health consequences for the infant.

Immediate newborn NAS signs include neurological excitability, gastrointestinal dysfunction, and autonomic dysfunction. Newborns with NAS are more likely than other babies to have low birthweight and respiratory complications. ONC believes the pediatric clinical health IT recommendations proposed in this rule (including Priority 8, which includes the linkage of health data in records of the mother and newborn) are important for supporting newborns at birth and as they grow and receive care in various settings. As such, we invite comment on:

- The effective use of health IT itself in support of the NAS use case as involves provider training, establishing

[55] To learn more about, and/or participate in, the ISA process, please visit *https://www.healthit.gov/isa/.*

[56] *https://www.medicaid.gov/federal-policy-guidance/downloads/smd18006.pdf.*

workflow, and other related safety and usability considerations.

- Existing and potential tools, such as decision support or clinical quality measurement, for supporting children with NAS and on the specific data elements related to the care of these children and use of these tools in practice.
- Identification of any related criteria and the respective corresponding proposed pediatric recommendation for the voluntary certification of health IT for use in pediatric care that supports the NAS use case including but not limited to recommendation number 8 noted above.

We welcome public comment on these health IT policies, functionalities and standards to support providers engaged in the treatment and prevention of OUD.

VII. Conditions and Maintenance of Certification

Section 4002 of the Cures Act requires the Secretary of HHS, through notice and comment rulemaking, to establish Conditions and Maintenance of Certification requirements for the Program. Specifically, health IT developers or entities must adhere to certain Conditions and Maintenance of Certification requirements concerning information blocking; appropriate exchange, access, and use of electronic health information; communications regarding health IT; application programming interfaces (APIs); real world testing for interoperability; attestations regarding certain Conditions and Maintenance of Certification requirements; and submission of reporting criteria under the EHR reporting program.

A. Implementation

To implement Section 4002 of the Cures Act, we propose an approach whereby the Conditions and Maintenance of Certification express both initial requirements for health IT developers and their certified Health IT Module(s) as well as ongoing requirements that must be met by both health IT developers and their certified Health IT Module(s) under the Program. If these requirements are not met, then the health IT developer may no longer be able to participate in the Program and/or its certified health IT may have its certification terminated. We propose to implement each Cures Act Condition of Certification with further specificity as it applies to the Program. We also propose to establish the Maintenance of Certification requirements for each Condition of Certification as standalone requirements. This approach would establish clear baseline technical and behavior Conditions of Certification requirements with evidence that the Conditions of Certification are continually being met through the Maintenance of Certification requirements.

B. Provisions

1. Information Blocking

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, not take any action that constitutes ''information blocking'' as defined in section 3022(a) of the PHSA (see 3001(c)(5)(D)(i) of the PHSA). We propose to establish this information blocking Condition of Certification in § 170.401. The Condition of Certification prohibits any health IT developer under the Program from taking any action that constitutes information blocking as defined by section 3022(a) of the PHSA and proposed in § 171.103.

We clarify that this proposed ''information blocking'' Condition of Certification and its requirements would be substantive requirements of the Program and would use the definition of ''information blocking'' established by section 3022(a) of the PHSA and as also proposed in § 171.103, as it relates to health IT developers of certified health IT. In addition to ONC's statutory authority for this Condition of Certification, the HHS Office of the Inspector General (OIG) has both investigatory and enforcement authority over information blocking and may issue civil money penalties for information blocking conducted by health IT developers of certified health IT, health information networks and health information exchanges. OIG may also investigate health care providers for information blocking for which health care providers could be subject to disincentives.

We refer readers to section VII.D of this proposed rule for additional discussion of ONC's enforcement of this and other proposed Conditions and Maintenance of Certification requirements. We also refer readers to section VIII of this proposed rule for our proposals to implement the information blocking provisions of the Cures Act, including proposed § 171.103.

We do not, at this time, propose any associated Maintenance of Certification requirements for this Condition of Certification.

2. Assurances

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, provide assurances to the Secretary, unless for legitimate purposes specified by the Secretary, that it will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA, or any other action that may inhibit the appropriate exchange, access, and use of electronic health information (EHI). We propose to implement this Condition of Certification and accompanying Maintenance of Certification requirements in § 170.402. As a Condition of Certification requirement, a health IT developer must comply with the Condition as recited here and in the Cures Act. We refer readers to section VIII of this proposed rule for the proposed reasonable and necessary activities specified by the Secretary, which constitute the exceptions to the information blocking definition.

We also propose to establish more specific Conditions and Maintenance of Certification requirements for a health IT developer to provide assurances that it does not take any action that may inhibit the appropriate exchange, access, and use of EHI. These proposed requirements serve to provide further clarity under the Program as to how health IT developers can provide such broad assurances with more specific actions.

a. Full Compliance and Unrestricted Implementation of Certification Criteria Capabilities

We propose, as a Condition of Certification, that a health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program (Program) conforms to the full scope of the certification criteria to which its health IT is certified. This has always been an expectation of ONC and users of certified health IT and, importantly, a requirement of the Program. We believe, however, that by incorporating this expectation and requirement as a Condition of Certification under the Program, there would be assurances, and documentation via the ''Attestations'' Condition and Maintenance of Certification requirements proposed in § 170.406, that all health IT developers fully understand their responsibilities under the Program, including not to take any action with their certified health IT that may inhibit the appropriate exchange, access, and use of EHI. To this point, certification criteria are designed and issued so that certified health IT can support interoperability and the appropriate exchange, access, and use of electronic health information.

We propose that, as a complementary Condition of Certification, health IT developers of certified health IT must provide an assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes. More specifically, developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Such actions may inhibit the appropriate access, exchange, or use of EHI and are therefore contrary to this proposed Condition of Certification and the statutory provision that it implements. While such actions are already prohibited under the Program (80 FR 62711), making these existing requirements explicit would ensure that health IT developers are required to attest to them on a regular basis pursuant to the Condition of Certification proposed in § 170.406, which will in turn provide additional assurances to the Secretary that developers of certified health IT support and do not inhibit appropriate access, exchange, or use of EHI.

By way of example, actions that would violate this aspect of the proposed Condition include failing to fully deploy or enable certified capabilities; imposing limitations (including restrictions) on the use of certified capabilities once deployed; or requiring subsequent developer assistance to enable the use of certified capabilities, contrary to the intended uses and outcomes of those capabilities (*see* 80 FR 62711). The Condition would also be violated were a developer to refuse to provide documentation, support, or other assistance reasonably necessary to enable the use of certified capabilities for their intended purposes (*see* 80 FR 62711). More generally, any action that would be likely to substantially impair the ability of one or more users (or prospective users) to implement or use certified capabilities for any purpose within the scope of applicable certification criteria would be prohibited by this Condition (*see* 80 FR 62711). Such actions may include imposing limitations or additional types of costs, especially if these were not disclosed when a customer purchased or licensed the certified health IT (*see* 80 FR 62711).

b. Certification to the ''Electronic Health Information Export'' Criterion

We propose, as a Condition of Certification requirement, that a health IT developer that produces and electronically manages EHI must certify health IT to the 2015 Edition ''electronic health information export'' certification criterion in § 170.315(b)(10). We discuss the proposed ''electronic health information (EHI) export'' criterion in section IV.B.4 of this proposed rule. Further, as a Maintenance of Certification requirement, we propose that a health IT developer that produces and electronically manages EHI must provide all of its customers of certified health IT with health IT certified to the functionality included in § 170.315(b)(10) within 24 months of a subsequent final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer. Consistent with these proposals, we also propose to amend § 170.550 to require that ONC–ACBs certify health IT to the proposed 2015 Edition ''EHI export'' when the health IT developer of the health IT presented for certification produces and electronically manages EHI.

As discussed in section IV.C.1 of this proposed rule, the availability of the capabilities in the proposed 2015 Edition ''EHI export'' certification criterion to providers and patients would promote access, exchange, and use of EHI to facilitate health care providers in switching practices and health IT systems and patients' electronic access to all their health information stored by a provider. As such, health IT developers with health IT certified to the proposed 2015 Edition ''EHI export'' certification criterion that is made available to its customers provides assurances that the developer is not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI.

c. Records and Information Retention

We propose that, as a Maintenance of Certification requirement, a health IT developer must, for a period of 10 years beginning from the date of certification, retain all records and information necessary that demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program. In other words, records and information should be retained starting from the date a developer first certifies health IT under the Program and applies separately to each unique Health IT Module (or Complete EHR, as applicable) certified under the Program. This retention of records is necessary to verify health IT developer compliance with Program requirements, including certification criteria and Conditions of Certification. We believe that 10 years is an appropriate period of time given that many users of certified health IT participate in various CMS programs, as well as other programs, that require similar periods of records retention. We also refer readers to section VII.D.3.c of this preamble for additional discussion of records access to information necessary to enforce the Conditions and Maintenance of Certification.

In an effort to reduce administrative burden, we also propose, that in situations where applicable certification criteria are removed from the Code of Federal Regulations before the 10 years have expired, records must only be kept for 3 years from the date of removal for those certification criteria and related Program provisions unless that timeframe would exceed the overall 10-year retention period. This ''3-year from the date of removal'' records retention period also aligns with the records retention requirements for ONC–ACBs and ONC–ATLs under the Program.

We encourage comment on these proposals and whether the proposed requirements can provide adequate assurances that certified health IT developers are demonstrating initial and ongoing compliance with the requirements of the Program; and thereby ensuring that certified health IT can support interoperability, and appropriate exchange, access, and use of EHI.

d. Trusted Exchange Framework and the Common Agreement—Request for Information

The Cures Act added section 3001(c)(9) to the PHSA, which requires the National Coordinator to work with stakeholders with the goal of developing or supporting a Trusted Exchange Framework and a Common Agreement (collectively, ''TEFCA'') for the purpose of ensuring full network-to-network exchange of health information. Section 3001(c)(9)(B) outlines a process for establishing a TEFCA between health information networks (HINs)—including provisions for the National Coordinator, in collaboration with the NIST, to provide technical assistance on implementation and pilot testing of the TEFCA. In accordance with section 3001(c)(9)(C), the National Coordinator shall publish the TEFCA on its website and in the **Federal Register**, as well as annually publish on its website a directory of the HINs that have adopted the Common Agreement and are capable of trusted exchange pursuant to the Common Agreement. The process, application, and construction of the

TEFCA are further outlined in section 3001(c)(9)(D), including requiring that the Secretary shall through notice and comment rulemaking, establish a process for HINs that voluntarily adopt the TEFCA to attest to such adoption. We request comment as to whether certain health IT developers should be required to participate in the TEFCA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. We would expect that such a requirement, if proposed in a subsequent rulemaking, would apply to health IT developers that have a Health IT Module(s) certified to any of the certification criteria in §§ 170.315(b)(1), (c)(1) and (c)(2), (e)(1), (f), and (g)(9) through (11); and provide services for connection to health information networks (HINs). These services could be routing EHI through a HIN or responding to requests for EHI from a HIN.

We have identified health IT developers that certify health IT to the criteria above because the capabilities included in the criteria support access and exchange of EHI. Therefore, we believe such health IT developers, as opposed to a health IT developer that only supports clinical decision support (§ 170.315(a)(9)) with its certified health IT, would be best suited to participate in the Trusted Exchange Framework and adhere to the Common Agreement. Similarly, we believe that many such health IT developers with the identified certified health IT would be in position, and requested by customers, to provide connection services to HINs. When such criteria are met (certified to the identified criteria above and actually providing connection services), participation in the Trusted Exchange Framework and adherence to the Common Agreement are consistent with this Condition and Maintenance of Certification as specified by the Cures Act, the intent of Congress to establish widespread interoperability and exchange of health information without information blocking, and supports ONC's responsibility, as established by the HITECH Act, to develop and support a nationwide health IT infrastructure that allows for the electronic use and exchange of information. More specifically, by participating in the Trusted Exchange Framework and adhering to the Common Agreement, these health IT developers provide assurances that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. For more information on the Trusted Exchange Framework and Common Agreement, please visit: *https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement.*

In consideration of this request for comment, we welcome comment on the certification criteria we have identified as the basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, other certification criteria that would serve as a basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, and whether the current structure of the Trusted Exchange Framework and Common Agreement are conducive to health IT developer participation and in what manner.

3. Communications

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, does not prohibit or restrict communication regarding the following subjects:

- The usability of the health information technology;
- The interoperability of the health information technology;
- The security of the health information technology;
- Relevant information regarding users' experiences when using the health information technology;
- The business practices of developers of health information technology related to exchanging electronic health information; and
- The manner in which a user of the health information technology has used such technology.

We propose to implement this Condition of Certification and its requirements in § 170.403. The Cures Act placed no limitations on the protection of the communications delineated above (referred to hereafter as ''protected communications''). As such, we propose to broadly interpret the subject matter of communications that are protected from developer prohibition or restriction as well as the conduct of developers that implicate the protection afforded to communications by this Condition of Certification and discuss this proposed approach in detail below. While we propose to implement a broad general prohibition against developers imposing prohibitions and restrictions on protected communications, we also recognize that there are circumstances where it is both legitimate and reasonable for developers to limit the sharing of information about their products. As such, we propose to allow developers to impose prohibitions or restrictions on protected communications in certain narrowly defined circumstances. In order for a prohibition or restriction on a protected communication to be permitted, we propose that it must pass a two-part test. First, the communication that is being prohibited or restricted must not fall within a class of communication about which no restriction or prohibition would ever be legitimate or reasonable—such as communications required by law, made to a government agency, or made to a defined category of safety organizations—and which we refer to hereafter as ''communications with unqualified protection.'' Second, to be permitted, a developer's prohibition or restriction must also fall within a prescribed category of circumstances for which we propose it is both legitimate and reasonable for a developer to limit the sharing of information about its products. This would be because of the nature of the relationship between the developer and the communicator or because of the nature of the information that is, or could be, the subject of the communication (referred to hereafter as ''permitted prohibitions and restrictions''). A restriction or prohibition that does not satisfy this two-part test will contravene this Condition of Certification. As discussed in more detail below, we propose that this two-part test strikes a reasonable balance between the need to promote open communication about health IT and related business practices, and the need to protect the legitimate interests of health IT developers and other entities.

a. Background and Purpose

This Condition of Certification addresses industry practices that severely limit the ability and willingness of health IT customers, users, researchers, and other stakeholders who use and work with health IT to openly discuss and share their experiences and other relevant information about the performance of health IT, including the ability of health IT to exchange health information electronically. These practices result in a lack of transparency around health IT that can contribute to and exacerbate patient safety risks, system security vulnerabilities, and product performance issues. As discussed below, these issues have been documented and reported on over a number of years.

The challenges presented by health IT developer actions that prohibit or restrict communications have been examined for some time. The problem was identified in a 2012 report by the Institute of Medicine of the National Academies (IOM) entitled ''Health IT and Patient Safety: Building Safer Systems for Better Care'' [57] (IOM Report). The IOM Report stated that health care providers, researchers, consumer groups other health IT users lack information regarding the functionality of health IT.[58] The IOM Report observed, relatedly, that many developers restrict the information that users can communicate about developers' products through nondisclosure clauses, confidentiality clauses, intellectual property protections, hold-harmless clauses, and other boilerplate contract language.[59] Importantly, the IOM Report found that such clauses discourage users from sharing information about patient safety risks related to health IT, which significantly limits the ability of health IT users to understand how health IT impacts patient safety.[60] The report stressed the need for health IT developers to enable the free exchange of information regarding the experience of using their health IT products, including the sharing of screenshots.[61]

Other close observers of health IT have similarly noted that broad restrictions on communications can inhibit the communication of information about errors and adverse events.[62] Concerns have also been raised by researchers of health IT products,[63] who emphasize that confidentiality and intellectual property provisions in contracts often place broad and unclear limits on authorized uses of information related to health IT, which in turn seriously impacts the ability of researchers to conduct and publish their research.[64]

The issue of health IT developers prohibiting or restricting communications about health IT has been the subject of a series of hearings by the Senate Committee on Health, Education, Labor and Pensions (HELP Committee), starting in the spring of 2015. During several hearings, stakeholders emphasized the lack of transparency around the performance of health IT in a live environment, noting that this can undermine a competitive marketplace, hinder innovation, and prevent improvements in the safety and usability of the technology.[65] [66] Additionally, the HELP Committee indicated serious concerns regarding the reported efforts of health IT developers to restrict, by contract and other means, communications regarding user experience, including information relevant to safety and interoperability.[67] When one Senator asked a panel of experts—which included a health IT developer—if there were any reasons for health IT contracts to have confidentiality clauses restricting users of health information technology from discussing their experience of using the health IT, all panel members agreed that such clauses should be prohibited.[68]

Prior to the HELP Committee hearings described above, the issue of developers prohibiting and restricting communications about the performance of their health IT was also addressed in House Energy and Commerce Committee hearings when committee members heard testimony and held discussions related to the Cures Act.[69] Commentary by witnesses at the hearings emphasized the need to ensure that health IT products are safe and encouraged the availability of information around health IT products to improve quality and ensure patient safety.

Developer actions that prohibit or restrict communications about health IT have also been the subject of investigative reporting.[70] A September 2015 report examined eleven contracts between health systems and major health IT developers and found that, with one exception, all of the contracts protected large amounts of information from being disclosed, including information related to safety and performance issues.[71] The report stated that broad confidentiality and intellectual property protection clauses were the greatest barriers to allowing the communication of information regarding potential safety issues and adverse events.[72]

Finally, ONC has itself been made aware of health IT developer contract language that purports to prohibit the disclosure of information about health IT, including even a customer's or user's opinions and conclusions about the performance and other aspects of the technology. Our extensive interactions with health care providers, researchers, and other stakeholders consistently indicate that such terms are not uncommon and that some developers may actively enforce them and engage in other practices to discourage communications regarding developers' health IT products and related business practices.

This proposed Condition of Certification is needed to significantly improve transparency around the functioning of health IT in the field. This will help ensure that the health IT ultimately selected and used by health care providers and others functions as expected, is less likely to have safety issues or implementation difficulties, enables greater interoperability of health information, and more fully allows users to reap the benefits of health IT utilization, including improvements in care and quality, and reductions in costs.

b. Condition of Certification Requirements

i. Protected Communications and Communicators

We propose that the protection afforded to communicators under this Condition of Certification would apply irrespective of the form or medium in which the communication is made. Developers must not prohibit or restrict communications whether written, oral, electronic or by any other method if they concern protected communications, unless permitted otherwise by this Condition of

[57] IOM (Institute of Medicine), *Health IT and Patient Safety: Building Safer Systems for Better Care* (2012). Available at *http://www.nationalacademies.org/hmd/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx.*

[58] *Id,* 195.

[59] *Ibid.*

[60] *Ibid.*

[61] *Ibid.*

[62] *See* Kathy Kenyon, *Overcoming Contractual Barriers to EHR Research,* Health Affairs Blog (October 14, 2015). Available at *http://healthaffairs.org/blog/2015/10/14/overcoming-contractual-barriers-to-ehr-research/.*

[63] *See* Hardeep Singh, David C. Classen, and Dean F. Sittig, *Creating an Oversight Infrastructure* for *Electronic Health Record-Related Patient Safety Hazards,* 7(4) Journal of Patient Safety 169 (2011). Available at *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3677059/.*

[64] Kathy Kenyon, *Overcoming Contractual Barriers to EHR Research,* Health Affairs Blog (October 14, 2015). Available at *http://healthaffairs.org/blog/2015/10/14/overcoming-contractual-barriers-to-ehr-research/.*

[65] HELP 6/10/15 pg 12; Available at *https://www.gpo.gov/fdsys/pkg/CHRG-114shrg25971/pdf/CHRG-114shrg25971.pdf.*

[66] HELP 3/17/15 pg 47; Available at *https://www.gpo.gov/fdsys/pkg/CHRG-114shrg93864/pdf/CHRG-114shrg93864.pdf.*

[67] HELP 7/23/15 pg 13, pg 27; Available at *https://www.help.senate.gov/hearings/achieving-the-promise-of-health-information-technology-information-blocking-and-potential-solutions.*

[68] HELP 7/23/15 pg 38; Available at *https://www.help.senate.gov/hearings/achieving-the-promise-of-health-information-technology-information-blocking-and-potential-solutions.*

[69] Energy and Commerce 7/17/14 pg 35; Available at *http://docs.house.gov/meetings/IF/IF16/20140717/102509/HHRG-113-IF16-20140717-SD008.pdf.*

[70] D Tahir, *POLITICO Investigation: EHR gag clauses exist—and, critics say, threaten safety,* Politico, August 27, 2015.

[71] *Ibid.*

[72] *Ibid.*

Certification. Similarly, this Condition of Certification does not impose any limit on the identity of the communicators that are able to benefit from the protection afforded, except that employees and contractors of a health IT developer may be treated differently when making communications that are not afforded unqualified protection under § 170.403(a)(2)(i). This Condition of Certification is not limited to communications by health IT customers (*e.g.,* providers) who have contracts with health IT developers. Entities or individuals who enter into agreements with a developer in connection with the developer's health IT—for example, a data analytics vendor who is required to sign a non-disclosure agreement before being granted access to the developer's health IT—would also be covered by the protection afforded to communicators under this Condition of Certification. Patients, health IT researchers, industry groups, and health information exchanges would be able to make protected communications about the health IT free of impermissible prohibitions or restrictions. Similarly, the Condition of Certification would also extend to potential customers of health IT who are provided with product or software demonstrations, irrespective of whether they proceed with the acquisition of the technology. Examples of other protected communications include, but are not limited to:

- A post made to an online forum;
- the sharing of screenshots, subject to certain proposed restrictions on their general publication;
- an unattributed written review by a health IT user;
- a quote given by a health care executive to a journalist;
- a presentation given at a trade show;
- a social media post;
- a product review posted on a video-sharing service such as YouTube;
- the statements and conclusions made in a peer-reviewed journal; and
- private communications made between health IT customers about the health IT.

ii. Protected Subject Areas

The Cures Act (and § 170.403(a)(1)) identifies a list of subject areas about which developers cannot prohibit or restrict communications. These subject areas address health IT performance and usability, health IT security, and the business practices related to exchanging EHI. For the reasons discussed below, we propose that the terms used to describe the subject areas should be construed broadly, consistent with the scope of communications that Congress specified in the Act. We encourage comment on whether the types of subject matter we identify below are adequate to protect the full range of communications contemplated by the Cures Act.

(A) Usability of Health Information Technology

The term ''usability'' is not defined in the Cures Act nor in any other relevant statutory provisions. In the National Institute of Standards and Technology (NIST) Usability Initiative, NIST describes ''usability'' of health IT by referencing the ISO[73] standard, ISO9241: Usability is ''the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.''[74] Separately, HIMSS[75] has recognized the following principles of software usability: Simplicity; Naturalness; Consistency; Forgiveness and Feedback; Effective Use of Language; Efficient Interactions; Effective Information Presentation; Preservation of Context; and Minimize Cognitive Load.[76] As these organizations have expressed, there are a multitude of factors that contribute to any judgment about ''usability,'' and any assessment about the usability of health IT should appropriately rest on the factors contributing to the effectiveness, efficiency, and performance offered. As such, we propose that the ''usability'' of health IT be construed broadly to include both an overall judgment on the ''usability'' of a particular health IT product, as well as any factor that contributes to usability. Factors of usability that could be the subject of protected communications include, but are not limited to: The user interface (*i.e.,* what a user sees on the screen, such as layout, controls, graphics and navigational elements); ease of use (*e.g.,* how many clicks); how the technology supports users' workflows; the organization of information; cognitive burden; cognitive support; error tolerance; clinical decision support; alerts; error handling; customizability; use of templates; mandatory data elements; the use of text fields; and customer support.

(B) Interoperability of Health Information Technology

Section 3000(9) of the PHSA, as amended by the Cures Act, provides a definition of ''interoperability'' that describes a type of health IT that demonstrates the necessary capabilities to be interoperable. For the purposes of this Condition of Certification, we propose that protected communications regarding the ''interoperability of health IT'' would include communications about whether a health IT product and associated developer business practices meet the interoperability definition described in section 3000(9) of the PHSA, including communications about aspects of the technology or developer that fall short of the expectations found in that definition. This will include communications about the interoperability capabilities of health IT and the practices of a health IT developer that may inhibit the access, exchange, or use of EHI, including information blocking.

(C) Security of Health IT

The security of health information technology is primarily addressed under the HIPAA Security Rule,[77] which establishes national standards to protect individuals' electronic protected health information (ePHI) that is created, received, maintained, or transmitted by a covered entity or business associate. Covered entities and business associates must ensure the confidentiality, integrity, and availability of all such ePHI; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.[78] HIPAA requires that health IT developers, to the extent that they are business associates of HIPAA-covered entities, implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.

We propose that the matters that fall within the topic of health IT security should be broadly construed to include any safeguards, whether or not required by the Security Rule, that may be implemented (or not implemented) by a developer to ensure the confidentiality,

[73] The International Organization for Standardization (ISO) is an international standard-setting organization that develops, publishes, and promotes proprietary, industrial, and commercial standards. For more information see *https://www.iso.org/home.html.*

[74] *See https://www.nist.gov/programs-projects/health-it-usability.*

[75] The Healthcare Information and Management Systems Society (HIMSS) is a not-for-profit organization that promotes the use of information technology in health care. For more information, see *http://www.himss.org/.*

[76] *See http://www.himss.org/what-ehr-usability.*

[77] 45 CFR part 160 and subparts A and C of part 164.

[78] 45 CFR part 160 and subparts A and E of part 164.

integrity, and security of the wider set of EHI (including ePHI), together with the health IT product's performance regarding security. For example, a developer may not prohibit or restrict a potential communicator from communicating about, without limitation:

- The approach to security adopted for the health IT at issue (*e.g.,* architectural approach or authentication methodology);
- the resilience of the health IT;
- identified security flaws in the developer's health IT; or
- the response to cyber threats or security breaches by the developer.

(D) User Experiences

The phrase ''user experience'' is not defined in the Cures Act nor in any other relevant statutory provisions. We propose to afford these terms their ordinary meaning. To qualify as a ''user experience,'' the experience must be one that is had by a user of health IT. However, beyond this, we do not propose to qualify the types of experiences that would receive protection under the Condition on the basis of the ''user experience'' subject area. This reflects the great variety of experiences that users may have with health IT and the often subjective nature of such experiences. Thus, we believe that if the user had the experience, the experience is relevant.

To illustrate the breadth of potential user experiences that would be protected by this Condition of Certification, we propose that communications about ''relevant information regarding users' experiences when using the health IT'' would encompass, for example, communications and information about a person or organization's experience acquiring, implementing, using, or otherwise interacting with health IT. This includes experiences associated with the use of the health IT in the delivery of health care, together with administrative functions performed using the health IT. User experiences would also include the experiences associated with configuring and using the technology throughout implementation, training, and in practice. Further, user experiences would include patients' and consumers' user experiences with consumer apps, patient portals, and other consumer-facing technologies. To be clear, a ''relevant user experience'' includes any aspect of the health IT user experience that could positively or negatively impact the effectiveness or performance of the health IT.

(E) Manner in Which a User Has Used Health IT

We propose that protected communications regarding the ''manner in which a user has used health IT'' would encompass any information related to how the health IT has been used in practice. This subject area largely overlaps with the matters covered under the ''user experience'' subject area but may include additional perspectives or details beyond those experienced by a user of health IT. Types of information that would fall within this subject area include but are not limited to:

- Information about a work-around implemented to overcome an issue in the health IT;
- customizations built on top of core health IT functionality;
- the specific conditions under which a user used the health IT, such as information about constraints imposed on health IT functionality due to implementation decisions; and
- information about the ways in which health IT could not be used or did not function as was represented by the developer.

(F) Business Practices Related to Exchange

We propose that the subject matter of ''developer business practices related to exchanging electronic health information'' should be broadly construed to include developer policies and practices that facilitate the exchange of electronic health information, and developer policies and practices that impact the ability of health IT to exchange health information. We further propose That the exchange of electronic health information encompasses the appropriate and timely sharing of electronic health information.

We propose that protected communications include, but are not limited to:

- The costs charged by a developer for products or services that support the exchange of electronic health information (*e.g.,* interface costs, API licensing fees and royalties, maintenance and subscription fees, transaction or usage-based costs for exchanging information);
- the timeframes and terms on which developers will or will not enable connections and facilitate exchange with other technologies, individuals, or entities, including other health IT developers, exchanges, and networks;
- the developer's approach to participation in health information exchanges and/or networks;
- the developer's licensing practices and terms as it relates to making available APIs and other aspects of its technology that enable the development and deployment of interoperable products and services; and
- the developer's approach to creating interfaces with third-party products or services, including whether connections are treated as ''one off'' customizations, or whether similar types of connections can be implemented at a reduced cost.

Importantly, we further propose that information regarding business practices related to exchanging electronic health information would include information about the switching costs imposed by a developer, as we are aware that the cost of switching health IT is a significant factor impacting health care providers adopting the most exchange-friendly health IT products that are available.

iii. Meaning of ''Prohibit or Restrict''

The terms ''prohibit'' and ''restrict'' are not defined in the Cures Act or in any other relevant statutory provisions. As discussed in detail below, communications can be prohibited or restricted through contractual terms or agreements (*e.g.,* non-disclosure agreements, non-disparagement clauses) as well as through conduct, including punitive or retaliatory business practices that are designed to create powerful disincentives to engaging in communications about developers or their products. Therefore, we propose that this Condition of Certification would not be limited to only formal prohibitions or restrictions (such as by means of contracts or agreements) and would encompass any conduct by a developer that would be likely to restrict a communication or class of communications protected by this Condition, as discussed in detail below.

The conduct in question must have some nexus to the making of a protected communication or an attempted or contemplated protected communication. That is, conduct by a developer that may be perceived as intimidating or punitive would not implicate this Condition of Certification unless that conduct was designed to directly or indirectly influence the making of a protected communication. Similarly, health IT contracts may include terms that govern the manner in which the parties conduct themselves, and those terms would not implicate this Condition of Certification unless the operative effect of a term was to restrict or prohibit a protected communication. For abundant clarity, we note that the fact that a customer's health IT product is not performing in the manner the customer expected, or in the manner that the developer promised, would not, in itself be evidence that the developer is engaging in conduct that restricts or prohibits a protected communication. Rather, a nexus must exist between the alleged poor performance and the making of (or attempting or contemplating to make) a protected communication.

We note that contractual prohibitions or restrictions on communications can, in limited circumstances, be legitimate and serve an important role in protecting proprietary information and intellectual property that are essential for health IT developers to innovate and compete. On this basis, we propose to permit certain types of prohibitions and restrictions, subject to strict conditions to ensure that they are narrowly tailored and do not restrict protected communications. These permitted prohibitions and restrictions are discussed in section VII.B.3.b.v below.

(A) Prohibitions or Restrictions Arising by Way of Contract

The principal way that health IT developers can control the disclosure of information about their health IT is through contractual prohibitions or restrictions. Such prohibitions or restrictions can arise in contractual provisions that address, for example, confidentiality obligations, intellectual property protections, hold-harmless requirements, nondisclosure obligations, non-compete obligations, and publicity rights.

There are different ways that contractual prohibitions or restrictions arise. In some instances a contractual prohibition or restriction will be expressed, and the precise nature and scope of the prohibition or restriction will be explicit from the face of the contract or agreement. For example, a contract will say that the health IT customer must not disclose screenshots of the health IT. However, more often, a contract will impose prohibitions or restrictions in less precise terms. For example, a health IT contract might use broad language when describing the information or materials that customers and users are forbidden from disclosing pursuant to a confidentiality clause, casting a vague net over the developer's ''proprietary'' information and purporting to cover information that may be neither confidential, secret, nor protected by law. A contract does not need to expressly prohibit or restrict a protected communication in order to have the effect of prohibiting or restricting that protected communication. The use of broad or vague language that obfuscates the types of communications that can and cannot be made may be treated as a prohibition or restriction if it has the effect of restricting legitimate communications about health IT.

Restrictions and prohibitions found in contracts used by developers to sell or license their health IT products can apply to customers directly and can require that the customer ''flow-down'' obligations onto the customer's employees, contractors, and other individuals or entities that use or work with the developer's health IT. Such contract provisions would not comply with this Condition of Certification if they prohibit or restrict protected communications. Prohibitions or restrictions on communications can also be found in separate nondisclosure agreements (NDAs) that developers require their customers—and in some instances the users of the health IT—to enter into in order to receive or access the health IT. We propose that such agreements are covered by this Condition of Certification. Finally, health IT developers typically may require third-party contractors used by their customers (such as a data analytics vendor engaged by a health care provider to analyze the provider's data) to enter into a NDA with the developer before commencing their contract activities. In some extreme cases, the employees of these third-party contractors are required to sign NDAs in their personal capacities. These NDAs typically include obligations that prohibit or restrict communications about the developer's health IT products, and we propose that any such prohibitions or restrictions within the context of protected communications as defined here would be subject to this Condition of Certification.

(B) Prohibitions or Restrictions That Arise by Way of Conduct

We are aware that some health IT developers engage in conduct that has the effect of prohibiting or restricting protected communications. This conduct may arise despite the developer's contract and/or business associate agreement being silent on, or even expressly permitting, the protected communication. The effect of such conduct can be significant, as health care providers are dependent on their health IT developer in order to receive critical software updates or other maintenance services, and sometimes have little bargaining power. Similarly, a third-party developer is dependent on a health IT developer's authorization in order to perform work in connection with the developer's health IT.

We propose that conduct that has the effect of prohibiting or restricting a protected communication would be subject to this Condition of Certification. We emphasize that, as discussed above, the conduct in question must have some nexus to the making of a protected communication or an attempted or contemplated protected communication. As such, developer conduct that was alleged to be intimidating, or health IT performance that was perceived to be substandard, would not, in and of itself, implicate this Condition of Certification unless there was some nexus between the conduct or performance issue and the making of (or attempting or threatening to make) a protected communication. Examples of conduct that could implicate this Condition of Certification include, but are not limited to:

- Taking steps to enforce, including by threatening to enforce, a right arising under contract that contravenes this Condition of Certification.
- Taking steps to enforce, including by threatening to enforce, a legal right that purports to prohibit or restrict a protected communication. This would include, for example, the making of threats, such as via a cease and desist letter, to a researcher who has made a protected communication.
- Employing a technological measure (within the meaning of 17 U.S.C. 1201) that a user would have to circumvent in order to make a protected communication, for example, a technological measure that a health IT user would need to circumvent in order to take a screenshot of the developer's health IT.
- Discouraging the making of protected communications by:
  - ○ Making threats against a health care customer (*e.g.,* by threatening to withhold the latest version of the developer's software) in response to the customer making or attempting to make a protected communication.
  - ○ Taking retaliatory action against a person or entity that has made a protected communication (*e.g.,* withholding support, delaying the provider's adoption of a new software release, or removing a provider from the developer's ''preferred customer'' list).
- Having policies that disadvantage persons or entities that make protected communications (*e.g.,* a policy that bars a provider from qualifying for the developer's ''preferred customer'' list if it shares screenshots in a manner protected by this Condition of Certification).
- Refusing to publish—or refusing to remove or delete—protected communications made in an online forum that the developer moderates or controls.

- Causing the removal or deletion of a protected communication from any publication (*e.g.,* a YouTube Copyright Take-down Notice that does not raise a legitimate copyright claim).

iv. Communications With Unqualified Protection

We propose, and discuss below, a narrow class of communications—consisting of five specific types of communications—that would receive unqualified protection from developer prohibitions or restrictions. With respect to communications with unqualified protection, a developer would be prohibited from imposing *any* prohibition or restriction. As discussed below, we propose that this narrow class of communications warrants unqualified protection because of the strength of the public policy interest being advanced by the communication and/or the sensitivity with which the identified recipient treats, and implements safeguards to protect the confidentiality and security of, the information received. A developer that imposes a prohibition or restriction on a communication with unqualified protection would fail the first part of the two-part test for allowable prohibitions or restrictions, and as such would contravene the Condition of Certification.

(A) Disclosures Required by Law

We propose that where a communication relates to subject areas enumerated in § 170.403(a)(1) and there are federal, state, or local laws that would require the disclosure of information related to health IT, developers must not prohibit or restrict in any way protected communications made in compliance with those laws. We note that we expect that most health IT contracts would allow for, or at the very least not prohibit or restrict, any communication or disclosure that is required by law, such as responding to a court or Congressional subpoena, or a valid warrant presented by law enforcement. We further propose that if required by law, a potential communicator should not have to delay any protected communication under this Condition of Certification. Furthermore, we propose that the reasonable limitations and prohibitions that are discussed below and permitted by § 170.403(a)(2) do *not* apply to these types of protected communications.

(B) Communicating Information About Adverse Events, Hazards, and Other Unsafe Conditions to Government Agencies, Health Care Accreditation Organizations, and Patient Safety Organizations

It is well established that there is a strong public interest in allowing open communication of information regarding health care hazards, adverse events, and unsafe conditions. Given the central role played by health IT in the delivery of care, information about health IT is a critical component of any investigation into the cause of hazards, adverse events, or unsafe conditions. On the basis of this public policy interest alone, we propose there is an overwhelming interest in ensuring that all communications about health IT that are necessary to identify patient safety risks, and to make health IT safer, not be encumbered by prohibitions or restrictions imposed by health IT developers that may affect the extent or timeliness of communications. In addition to the public policy interest in promoting uninhibited communications about health IT safety, the recognized communication channels for adverse events, hazards, and unsafe conditions provide protections that help ensure that any disclosures made are appropriately handled and kept confidential and secure. Indeed, the class of recipients to which the information can be communicated under this category of communications with unqualified protection should provide health IT developers with comfort that there is very little risk of such communications prejudicing the developer's intellectual property rights. For example, government agencies impose appropriate controls on information they receive, mitigating any risk that developers may feel arises from the disclosure of information about their health IT. Similarly, accrediting bodies for health care delivery observe strict confidentiality policies for information received or developed during the accreditation process and in connection with complaints received.

Finally, the Patient Safety and Quality Improvement Act of 2005 (PSQIA) [79] provides for privilege and confidentiality protections for information that meets the definition of patient safety work product (PSWP). This means that PSWP may only be disclosed as permitted by the PSQIA and its implementing regulations. We clarify that to the extent activities are conducted in accordance with the PSQIA, its implementing regulation, and section 4005(c) of the Cures Act, no such activities shall be construed as constituting restrictions or prohibitions that contravene this Condition of Certification.

We understand that the nature of the information about health IT that would ordinarily be disclosed by a health care provider when reporting an adverse event, hazard, or unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations, would not ordinarily contain intellectual property or trade secrets. Notwithstanding this, in light of the public policy interest and established reporting mechanisms described above, we do not consider the potential inclusion of intellectual property or trade secrets in the communication should prohibit or restrict a health care provider from making a complete and timely report. For example, proposed § 170.403(a)(2)(ii)(D) permits developers to impose certain restrictions on the general publication of screenshots, but we do not consider that such restrictions should be permitted when the communication is made for one of the purposes, and to one of the recipients, identified in § 170.403(a)(2)(i)(B).

We seek comment on whether the unqualified protection afforded to communications made to a patient safety organizations about adverse events, hazards, and other unsafe conditions should be limited. Specifically, we seek comment on whether the unqualified protection should be limited by the nature of the patient safety organization to which a communication can be made, or the nature of the communication that can made—such as limiting to only material that was created as PSWP.

(C) Communicating Information About Cybersecurity Threats and Incidents to Government Agencies

We propose that if health IT developers were to impose prohibitions or restrictions on the ability of any person or entity to communicate information about cybersecurity threats and incidents to government agencies, such conduct would not comply with this Condition of Certification. Government agencies such as the United States Computer Emergency Readiness Team (US–CERT) respond to and protect both the government and private industry from cyber threats. Their work helps protect the entire health care system from cybersecurity threats and relies on the timely reporting of security issues and vulnerabilities by health care

[79] Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b–21–b–26 (Pub. L. 109–41).

providers and health IT users. These agencies impose appropriate controls on information they receive, which mitigates any risk that developers may feel arises from the disclosure of information about their health IT. The US–CERT, for example, provides secure forms for such reporting, and we are confident that reporting security incident information to US–CERT and other government agencies would be unlikely to pose any threat to health IT developer intellectual property or trade secrets. Additionally, the information likely reported regarding such an incident would generally not reveal trade secrets. Where circumstances may require collection of more sensitive and confidential information related to a developer's intellectual property, we believe that appropriate protections would likely apply and that the public benefit of thoroughly investigating and addressing cybersecurity issues outweighs any potential harm.

Communications about security issues related to health IT may alert nefarious individuals or entities to the existence of a security vulnerability which could be exploited before a developer has time to fix the vulnerability. However, we propose that this concern must be balanced against the imperative of ensuring that health IT customers are aware of security vulnerabilities so that they can respond by deploying reactive measures independent of the developer, such as ceasing health information exchange with a compromised system. We seek comment on whether it would be reasonable to permit health IT developers to impose limited restrictions on communications about security issues so as to safeguard the confidentiality, integrity, and security of eHI. For example, should health IT developers be permitted to require that health IT users notify the developer about the existence of a security vulnerability prior to, or simultaneously with, any communication about the issue to a government agency?

(D) Communicating Information About Information Blocking and Other Unlawful Practices to a Government Agency

As in the circumstances described above, we believe that the public benefit associated with the communication of information to government agencies on information blocking, or any other unlawful practice, outweighs any concerns developers might have about the disclosure of information about their health IT. We believe that reporting information blocking, as well as other unlawful practices, to a government agency would not cause an undue threat to a health IT developer's intellectual property or trade secrets. Generally speaking, agencies collecting reports would protect all information received and keep it confidential to the extent permitted by law.

(E) Communicating Information About a Health IT Developer's Failure To Comply With a Condition of Certification or Other Program Requirement

We propose that the benefits to the public and to users of health IT of communicating information about a health IT developer's failure to comply with a Condition of Certification or other Program requirement (45 CFR part 170) justify prohibiting developers of health IT from placing any restrictions on such protected communications. Information regarding the failure of a health IT product to meet any Condition of Certification or other Program requirement is vital to the effective performance and integrity of the Program, which certifies that health IT functions consistent with its certification. While the current procedures for reporting issues with certified health IT encourage providers to contact developers in the first instance to address certification issues, users of health IT should not hesitate to contact ONC-Authorized Certification Bodies (ONC–ACBs), or ONC itself, if the developer does not provide an appropriate response, or the matter is of a nature that should be immediately reported to an ONC–ACB or to ONC.

v. Permitted Prohibitions and Restrictions

We propose that, *except for communications with unqualified protection discussed above and enumerated in § 170.403(a)(2)(i),* health IT developers would be permitted to impose certain narrow kinds of prohibitions and restrictions discussed below and specified in § 170.403(a)(2)(ii). We believe this policy strikes a reasonable balance between the need to promote open communication about health IT and related business practices and the need to protect the legitimate interests of health IT developers and other entities. Specifically, with the exception of communications with unqualified protection, developers would be permitted to prohibit or restrict the following communications, subject to certain conditions:

- Communications of their own employees;
- Disclosure of non-user-facing aspects of the software;
- Certain communications that would infringe the developer's or another person's intellectual property rights;
- Publication of screenshots in very narrow circumstances; and
- Communications of information that a person or entity knows only because of their participation in developer-led product development and testing.

As discussed in detail in the sections that follow, the proposed Condition of Certification carefully delineates the circumstances under which these types of prohibitions and restrictions would be permitted, including certain associated conditions that developers would be required to meet. To be clear, any prohibition or restriction not expressly permitted would violate the Condition. Additionally, it would be the developer's burden to demonstrate to the satisfaction of ONC that the developer has met all associated requirements. Further, as an additional safeguard, we propose that where a developer seeks to avail itself of one of the permitted types of prohibitions or restrictions, the developer must ensure that potential communicators are clearly and explicitly notified about the information and material that can be communicated, and that which cannot. We propose this would mean that the language of health IT contracts must be precise and specific. Contractual provisions or public statements that support a permitted prohibition or restriction on communication should be very specific about the rights and obligations of the potential communicator. Contract terms that are vague and cannot be readily understood by a reasonable health IT customer will not benefit from the qualifications to this Condition of Certification outlined below.

(A) Developer Employees and Contractors

We recognize that health IT developer employees, together with the entities and individuals who are contracted by health IT developers to deliver products and/or services (such as consultants), may be exposed to highly sensitive, proprietary, and valuable information in the course of performing their duties. We also recognize that the proper functioning of a workforce depends, at least in part, on the ability of an employer to regulate how and when the organization communicates information to the public, and that employees owe confidentiality obligations to their employers. We propose that on this basis, developers are permitted to impose prohibitions or restrictions on the communications of employees and contractors to the extent that those communications fall outside of the class of communications with unqualified protection as discussed above.

(B) Non-User-Facing Aspects of Health IT

The purpose of this Condition of Certification is to ensure that health IT users and other potential communicators are not restrained in their ability to communicate—publicly or privately—about certain protected subject areas. We propose that this purpose can generally be achieved without communicators disclosing information about those parts of health IT that are legally protected trade secrets. As such, we propose this Condition of Certification will permit health IT developers to impose prohibitions and restrictions on communications that are not communications with unqualified protection to the extent necessary to ensure that communications do not disclose ''non-user-facing aspects of health IT.''

A ''non-user-facing aspect of health IT'' is, for the purpose of this Condition of Certification, an aspect of health IT that is not a ''user-facing aspect of health IT.'' A ''user-facing aspect of health IT'' means those aspects of health IT that that are disclosed and evident to anyone running, using, or observing the operation of health IT. That is, a user-facing aspect of health IT comprises those aspects of the health IT that are manifest in how the health IT software works. User-facing aspects of health IT include the design concepts and functionality that is readily ascertainable from the health IT's user interface and screen display. They do not include those parts of the health IT that are not exposed to persons running, using, or observing the operation of the health IT. We propose that non-user-facing aspects of health IT would include source and object code, software documentation, design specifications, flowcharts, and file and data formats. We welcome comments on whether these and other aspects of health IT should be treated as not being user-facing.

For clarity, we note that the terminology of ''user-facing aspects of health IT'' is not intended to afford only health IT users with specific protections against developer prohibitions or restrictions on communications. Rather, the terminology is agnostic as to the identity of the communicator and is instead focused on describing those aspects of health IT that are readily ascertainable from the health IT's user interface and screen display. Numerous other potential communicators will also be exposed to ''user-facing aspects of health IT,'' such as third-party contractors, health information exchange organizations, recipients of a software demonstration, and trade groups or researchers that observe the operation of health IT in the field.

We propose that this approach reasonably implements the Cures Act, which, in direct response to strict confidentiality obligations, broad intellectual property clauses, and non-disclosure provisions in EHR contracts, identified a list of protected subject areas for disclosure (enumerated at section 3001(c)(5)(D)(iii) of the PHSA) that largely targeted the aspects of health IT that are apparent to, and known by, individuals and entities that use or interact with health IT. We propose that if a health IT user were prohibited from describing the user-facing aspects of their health IT product, they could not sensibly communicate useful information about the usability or interoperability of the product, or their experiences as a health IT user. These subject areas are fundamentally tied to the way that the health IT product works, its design, and its functionality.

Protecting the communication of ''user-facing aspects of health IT'' is also consistent with the treatment of software products under trade secret law, where the public-facing aspects of software products are not generally considered secret because they are evident to anyone running the software program. Moreover, this approach is appropriate given the manner in which health IT is deployed and used by health IT customers. Unlike software products that are deployed and used in a cloistered setting where access to the software is highly restricted, health IT is typically deployed in a setting in which the operation of the health IT can be readily observed by a wide range of persons. Health IT used in a physician's consulting room can be observed by the patient. Health IT deployed in a hospital can be observed by numerous individuals in addition to those who are ''authorized users'' of the health IT system, including, for example, the patient, the patient's family, volunteer staff, law enforcement, and clergy. As such, because health IT is of a nature that license terms or nondisclosure obligations do not act as a genuine control over the disclosure of those aspects of the software that are ''user-facing,'' communications about such aspects should be afforded protection from developer prohibitions and restrictions under this proposed Condition of Certification.

(C) Intellectual Property

Many aspects of health IT—including software and documentation—will contain intellectual property that belongs to the health IT developer (or a third party) and is protected by law. Health IT products may have portions in which copyrighted works exist, or that are subject to patent protection. As in other technology sectors, health IT developers place a high value on their intellectual property and go to significant lengths to protect it, including intellectual property provisions in their health IT contracts.

This Condition of Certification is not intended to operate as a *de facto* license for health IT users and others to act in any way that might infringe the legitimate intellectual property rights of developers. Indeed, we propose that health IT developers are permitted to prohibit or restrict communications that would infringe their intellectual property rights so long as the communication in question is not a communication with unqualified protection. However, any prohibition and restriction imposed by a developer must be no broader than legally permissible and reasonably necessary to protect the developer's legitimate intellectual property interests. We are aware that some health IT contracts contain broad intellectual property provisions (and related terms, such as nondisclosure provisions) that purport to prevent health IT customers and users from using copyright material in ways that are lawful. On this basis, while we are providing an exception for the protection of intellectual property interests, we want to clarify that under this Condition of Certification health IT developers are not permitted to prohibit or restrict, or purport to prohibit or restrict, communications that would be a ''fair use'' of any copyright work comprised in the developer's health IT. That is, a developer is not permitted to prohibit or restrict communications under the guise of copyright protection (or under the guise of a confidentiality or non-disclosure obligation) when the communication in question makes a use of the copyright material in a way that would qualify that use as a ''fair use.''[80]

We welcome comments on whether an appropriate balance has been struck between protecting legitimate intellectual property rights of developers and ensuring that health IT customers, users, researchers, and other stakeholders who use and work with health IT can openly discuss and share their experiences and other relevant

[80] *See* 17 U.S.C. 107.

information about the performance of health IT.

(D) Faithful Reproductions of Health IT Screenshots

We propose that health IT developers generally would not be permitted to prohibit or restrict communications that disclose screenshots of the developer's health IT. We consider screen displays an essential component of health IT performance and usability, and their reproduction may be necessary in order for a health IT user or other health IT stakeholder to properly make communications about the subject matters enumerated in § 170.403(a)(1). We acknowledge that some health IT developers have historically and aggressively sought to prohibit the disclosure of such communications. We consider that developers may benefit from screen displays being faithfully reproduced so that health IT users and other stakeholders can form an objective opinion on any question raised about usability in communications protected by this proposed Condition of Certification. Moreover, we consider that the reproduction of screenshots in connection with the making of a communication protected by this Condition of Certification would ordinarily represent a ''fair use'' of any copyright subsisting in the screen display, and developers should not impose prohibitions or restrictions that would limit that fair use.

Notwithstanding the above, we propose to permit certain prohibitions and restrictions on the communication of screenshots. Except in connection with communications with unqualified protection, developers would be permitted to impose certain restrictions on the disclosure of screenshots, as described below.

In order to ensure that disclosures of screenshots are reasonable and represent a faithful reproduction of the developer's screen design and health IT, we propose that developers would be permitted to prevent communicators from altering screenshots, other than to annotate the screenshot or to resize it for the purpose of publication. We consider this a reasonable limitation on the disclosure of screenshots and one that would help developers' health IT avoid being misrepresented by communicators seeking to make a communication protected by this proposed Condition of Certification.

We also propose that health IT developers could impose restrictions on the disclosure of a screenshot on the basis that it would infringe third-party intellectual property rights (on their behalf or as required by license). However, to take advantage of this exception, the developer would need to first put all potential communicators on sufficient written notice of those parts of the screen display that contain trade secrets or intellectual property rights and cannot be communicated, and would still need to allow communicators to communicate redacted versions of screenshots that do not reproduce those parts.

Finally, we also recognize that health IT developers may have obligations under HIPAA as a business associate and that it would be reasonable for developers to impose restrictions on the communication of screenshots that contain protected health information, provided that developers permit the communication of screenshots that have been redacted to conceal protected health information, or the relevant individual's consent or authorization had been obtained.

(E) Testing and Development

We are aware that some health IT developers expose aspects of their health IT to health care providers and others for the purpose of testing and development prior to a product's ''general availability'' release. Such disclosures may relate to beta releases that are shared with certain customers for testing prior to the software being made generally available to the market, or may be made as part of a joint-venture or cooperative development process. In these circumstances, we propose that a health IT developer would be justified in keeping information about its health IT confidential, and we do not intend that the protection afforded to communicators under this Condition of Certification would allow disclosures of this information. This permitted prohibition or restriction would allow developers to seek appropriate intellectual property protection and freely discuss novel, ''unreleased'' product features with their customer base, which has significant public policy benefits for research and innovation in the health IT industry.

As with the other allowable restrictions listed above, we propose that this permitted restriction would be limited and does not apply to communications which are communications with unqualified protection as described above and specified in § 170.403(a)(2)(i). For example, information that is learned as part of development and testing, such as the hard-coding of test procedure processes that raise serious patient safety concerns, could be communicated for one of the limited purposes specified in § 170.403(a)(2)(i) if the software is certified or released to market. We propose that this permitted restriction would also not apply to communications about the released version of the health IT once the health IT has been released to market or has been certified, provided that the communications otherwise meet all other requirements to be afforded protection under this Condition of Certification and the information communicated could be discovered by any ordinary user of the health IT.

For example, a health IT developer and a large health system enter into an agreement for members of the health IT developer's engineering team to work with members of the health system's clinical team to develop a customization for the system's use of the developer's EHR. In order to properly protect any intellectual property rights, or proprietary information, arising from this work, the developer and health system enter into a contract which imposes on the system and affected members of its clinical team strict nondisclosure related to testing and development of the health IT. This would be reasonable and would not contravene this Condition of Certification, provided that: (1) The nondisclosure obligations were narrowly targeted toward the work product associated with the testing and development; and (2) the obligations ceased immediately upon any resultant software being deployed in the health system, to the extent that the information fell within one of the subject areas enumerated in § 170.403(a)(1) and would be apparent to an ordinary user of the health IT.

To ensure that this permitted prohibition/restriction is not abused, such as by maintaining a product in beta release for an indefinite or lengthy period of time, we request comment on whether we should limit the time this protection would apply for testing purposes. This could be no longer than a year after release of a product or update. We also request comment on whether we should set specific parameters for covered testing. For example, we note above our expectations that a product would be shared with *certain* customers for testing prior to the software being made *generally available* to the market. As such, for this permitted prohibition/restriction to apply, should we more specifically limit the extent a product can be distributed to customers for testing purposes?

c. Maintenance of Certification Requirements

We propose that to maintain compliance with this Condition of Certification a health IT developer must not establish or enforce any contract or agreement provision that contravenes this Condition of Certification. We are aware that some developers currently have in place health IT contracts that contain provisions that contravene this proposed Condition of Certification because they impose impermissible prohibitions or restrictions on communications. In some instances, the provisions in question will be expressly at odds with this Condition, imposing obligations on health IT customers, or creating rights in favor of the developer, that prohibit or restrict communications that are protected. In other instances, a contract will include a provision that contravenes this Condition because it has been drawn in such broad terms—such as an overly-expansive definition of confidential information—that a reasonable reader of the provision would consider the making of a communication protected by this Condition a breach of the contract.

Health IT contracts are typically for a significant duration—*e.g.,* 5 years or more—or include an automatic renewal whereby the then current terms roll over for any renewal period. The implementation of this proposed Condition of Certification cannot therefore wait until health IT contracts that contravene this Condition expire in the ordinary course. As such, we are requiring that health IT developers take immediate steps to become in compliance with this Condition of Certification.

We propose that a health IT developer must notify all customers and those with which it has contracts/agreements, within six months of the effective date of a subsequent final rule for this proposed rule, that any communication or contract/agreement provision that contravenes this Condition of Certification will not be enforced by the health IT developer. Further, we propose that this notice would need to be provided annually up to and until the health IT developer amends the contract or agreement to remove or make void any contractual provision that contravenes this Condition of Certification. We further propose as a Maintenance of Certification requirement in § 170.405(b)(2) that health IT developers must amend their contracts or agreements to remove or make void any provisions that contravene the Condition of Certification within a reasonable period of time, but not later than two years from the effective date of a subsequent final rule for this proposed rule.

We believe this is an appropriate approach as we understand that health IT developers are in regular contact with their customers, and so the provision of a notice that satisfies this requirement should not present an undue burden for a developer. We would also expect that developers have kept good records of nondisclosure agreements that they have entered into with other organizations or individuals, such as third-party developers, and can communicate with those organizations or individuals as necessary to satisfy this requirement. In the event that a health IT developer cannot, despite all reasonable efforts, locate an entity or individual that previously entered into an agreement with the developer that prohibits or restricts communications protected by this Condition, the developer would not be in contravention of this Condition so long as it takes no step to enforce the prohibition or restriction. For clarity, we do not propose that health IT developers be required to furnish to ONC or their ONC–ACB copies of notices made to customers, or copies of contracts or agreements revised, in satisfaction of this Maintenance of Certification requirement, although those communications may be requested by ONC or an ONC–ACB in the usual course of business. To this point, under the ''Enforcement'' section of this proposed rule (VII.D), we describe our general enforcement approach outlining a corrective action process for ONC to review instances where Conditions and Maintenance of Certification requirements are not being met by a health IT developer under the Program.

We note that another approach we considered proposing would have been to require that developers amend their current health IT contracts immediately. We have, however, relied on the proposed requirement that developers not enforce contractual terms that contravene this proposed Condition of Certification until they can amend their contracts in a reasonable period of time, but not later than two years from the effective date of a subsequent final rule for this proposed rule. We seek comment on whether this is an adequate approach to removing prohibitions and restrictions on protected communications and ensuring that health IT customers, users, researchers, and other stakeholders are aware of their right to engage in such communications notwithstanding existing contracts or agreements to the contrary.

4. Application Programming Interfaces

As a Condition of Certification (and Maintenance thereof) under the Program, the Cures Act requires health IT developers to publish APIs that allow ''health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.'' The Cures Act's API Condition of Certification also states that a developer must, through an API, ''provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.''

The Cures Act's API Condition of Certification includes several key phrases and requirements for health IT developers that go beyond just the technical functionality of the products they present for certification. In this section of the preamble we outline our proposals to implement the Cures Act's API Condition of Certification in order to provide compliance clarity for health IT developers.

These proposals include new standards, new implementation specifications, and a new certification criterion as well as detailed Conditions and Maintenance of Certification requirements. We also propose to modify the Base EHR definition. We note that health IT developers should also consider these proposals in the context of what could warrant review from an information blocking perspective in so far as action (or inaction) that would be inconsistent with this proposed rule's API Conditions and Maintenance of Certification requirements.

a. Statutory Interpretation and API Policy Principles

One of the most significant phrases in the Cures Act's API Condition of Certification concerns the deployment and use of APIs ''without special effort.'' Specifically, the Cures Act requires health IT developers to publish APIs and allow health information from such technology ''to be accessed, exchanged, and used without special effort.'' In this context, we interpret the ''effort'' exerted (*i.e.,* by whom) to be focused on the API users, which could include third-party software developers, the health care providers that acquired this API technology, and patients, health care providers, and payers that use apps/services that connect to API technology.

As we considered the meaning and context associated with the phrase ''without special effort'' and what would make APIs included in certified health IT truly ''open,'' we focused on key attributes that could be used to refine our interpretation and guide our proposals. We interpret ''without special effort'' to require that APIs, and the health care ecosystem in which they are deployed, have three attributes: *Standardized, transparent,* and *pro-competitive.* Each of these attributes is briefly described in more detail below and all of our subsequent proposals address one or a combination of these attributes.

- *Standardized*—meaning that all health IT developers seeking certification would have to implement the same technical API capabilities in their products (using modern, computing standards such as RESTful interfaces and XML/JSON). Technical consistency and implementation predictability are fundamental to scale API-enabled interoperability and reduce the level of custom development and costs necessary to access, exchange, and use health information. Further, from a regulatory standpoint, health IT developers would gain certainty in regards to pre-certification testing requirements and post-certification ''real world testing'' expectations. Equally, from an industry standpoint, a consistent and predictable set of API functions would provide the health IT ecosystem with known technical requirements against which ''app'' developers and other innovative services can be built.
- *Transparent*—meaning that all health IT developers seeking certification would need to make the specific business and technical documentation necessary to interact with the APIs in production freely and publicly accessible. Such transparency and openness is commonplace in many other industries and has fueled innovation, growth, and competition.
- *Pro-competitive*—meaning that all health IT developers seeking certification would need to abide by business practices that promote the efficient access, exchange, and use of EHI to support a competitive marketplace that enhances consumer value and choice. Moreover, health care providers should have the sole authority and autonomy to unilaterally permit third-party software developers to connect to the API technology they have acquired. In other words, health IT developers must not interfere with a health care provider's use of their acquired API technology in any way, especially ways that would impact its equitable access and use based on (for example) another software developer's size, current client base, or business line. It also means that developers (together with health care providers that deploy APIs) are accountable to patients who, as consumers of health care services, have paid for their care and the information generated from such care. Thus, patients should be able to access their EHI via any API-enabled app they choose without special effort, including without incurring additional costs and without encountering access requirements that impede their ability to access their information in a persistent manner.

b. Key Terms

To clearly convey the stakeholders on which our proposals focus and are meant to support, we propose to use the following terms to reflect these meanings and/or roles:

- The term ''*API technology*'' (with a lowercase ''t'') generally refers to the capabilities of certified health IT that fulfill the API-focused certification criteria adopted or proposed for adoption at 45 CFR 170.315(g)(7) through (g)(11).
- ''*API Technology Supplier*'' refers to a health IT developer that creates the API technology that is presented for testing and certification to any of the certification criteria adopted or proposed for adoption at 45 CFR 170.315(g)(7) through (g)(11). We propose to adopt this term in § 170.102.
- ''*API Data Provider*'' refers to the organization that deploys the API technology created by the ''API Technology Supplier'' and provides access via the API technology to data it produces and electronically manages. In some cases, the API Data Provider may contract with the API Technology Supplier to perform the API deployment service on its behalf. However, in such circumstances, the API Data Provider retains control of what and how information is disclosed and so for the purposes of this definition is considered to be the entity that deploys the API technology. We propose to adopt this term in § 170.102.
- ''*API User*''—refers to persons and entities that use or create software applications that interact with the APIs developed by the ''API Technology Supplier'' and deployed by the ''API Data Provider.'' An API User includes, but is not limited to, third-party software developers, developers of software applications used by API Data Providers, patients, health care providers, and payers that use apps/services that connect to API technology. We propose to adopt this term in § 170.102.

We also use:

- The term ''*(g)(10)-certified API*'' for ease of reference throughout the preamble to refer to health IT certified to the certification criterion proposed for adoption in 45 CFR 170.315(g)(10).
- The term ''*app*'' for ease of reference to describe any type of software application that would be designed to interact with the (g)(10)-certified APIs. This generic term is meant to include, but not be limited to, a range of applications from mobile and browser-based to comprehensive business-to-business enterprise applications administered by third parties.

c. Proposed API Standards, Implementation Specifications, and Certification Criterion

APIs can be thought of as a set of commands, functions, protocols, and/or tools published by one software developer (''software developer A'') that enable other software developers (X, Y, and Z) to create programs and applications that interact with A's software without needing to know the ''internal'' workings of A's software. APIs can facilitate more seamless access to health information and it is important to note for context that ONC adopted three 2015 Edition certification criteria that specified API capabilities for Health IT Modules (criteria adopted in 45 CFR 170.315(g)(7), (g)(8), and (g)(9)). The following sections detail our proposals to adopt standards, implementation specifications, and a new API certification criterion. Together, these proposals account for the technical requirements we propose to associate with the Cures Act's API Condition of Certification and are reinforced through the condition's policy proposals.

i. Proposed Adoption of FHIR DSTU2 Standard

Overall, and on balance, we have structured our standards and implementation specifications proposals to best meet the health IT industry where it is most prepared to comply today. As a result, we propose to adopt the HL7® Fast Healthcare Interoperability Resources (FHIR®) standard as a foundational standard within our suite of proposals. Specifically, we propose to adopt FHIR Draft Standard for Trial Use (DSTU) 2 (hereafter referred to as ''FHIR Release 2'') as a baseline standard conformance requirement. In so doing, we can work with industry to support a conformance testing infrastructure for a full suite of proposals focused on one FHIR release (its associated implementation specifications) and complementary security and app registration protocols, compared to numerous versions.[81]

The 2015 Edition final rule did not include specific standards or implementation specifications to describe the way in which APIs needed to be designed to meet § 170.315(g)(8). Instead, we specified a functional certification criterion and encouraged the industry to coalesce around a standardized specification for its API functionality, such as the FHIR standard. We did, however, require health IT developers to make their technical API documentation publicly available and we subsequently made such information accessible via the CHPL.

Upon reviewing health IT developers certified to § 170.315(g)(8), approximately 32% have published via the CHPL that they are using FHIR, specifically FHIR Release 2, as of mid-September 2018. Additionally, nearly 51% of health IT developers appear to be using a version of FHIR and OAuth 2.0 together. We also note that when viewed from the perspective of how many providers are served by these FHIR implementers, we estimate that approximate 87% of hospitals and 57% of clinicians are served by developers with a FHIR Release 2 API and 87% of hospitals and 69% of clinicians are served by developers with a FHIR API of any version. In the years since the 2015 Edition final rule, industry stakeholders have made rapid progress to advance the FHIR standard. This includes substantial investments in industry pilots, specification development led through the Argonaut Project[82] production deployment of APIs conformant to FHIR Release 2 following the Argonaut specifications, and the support for FHIR Release 2 in Apple's iOS 11.3, which includes a new ''health records'' app for the iPhone based on these specifications.[83] Therefore, the industry is well prepared and ready to adopt the FHIR standard.

Thus, we propose to adopt FHIR Release 2 as the baseline standard in a new API standards section of our rules at 45 CFR 170.215(a)(1). Additionally, as discussed in further detail below, we reference FHIR Release 2 for use in the new API certification criterion proposed for adoption in § 170.315(g)(10).

Although FHIR Release 3 is published and some health IT developers have included varied support for it in their product(s) at this time, there is limited evidence that its production deployment is as widespread as FHIR Release 2. Thus, we believe that FHIR Release 2 is the most appropriate version to propose to adopt as part of proposed § 170.315(g)(10)'s conformance requirements. This approach would provide a stable and consistent direction in which the industry can go when it comes to deploying (g)(10)–certified APIs that support data access to the USCDI. FHIR Release 2 best reflects the industry's current maturity and implementation readiness, it has been more rigorously tested, and it is largely implemented in most 2015 Edition health IT systems that have and are being deployed in production. Thus, the incremental burden for many health IT developers to get certified to the proposed criterion in § 170.315(g)(10) would be largely limited to the added security and registration conformance requirements we have proposed to include. We recognize, however, that some health IT developers certified to § 170.315(g)(8) chose not to use FHIR and will have more substantial changes to make in order to meet this proposal.

Additionally, FHIR Release 4 has now been published[84] and updated associated implementation specifications are expected to follow. FHIR Release 4 has several key improvements, including certain foundational aspects in the standard and ''FHIR resources'' designated as ''normative'' for the first time. This will lead to acycle of more mature US FHIR Core profiles aligned with Release 4 and additional implementation guidance that explicitly specifies how to handle populations of patient data (batch exports) via FHIR to more efficiently enable population and learning health system-oriented services. Likewise, from an industry update trajectory, we believe that FHIR Release 4's normative resources will be compelling from a maturity and stability perspective such that many health IT developers will either rapidly progress to FHIR Release 4 from Release 3 or skip wide-scale production deployment of FHIR Release 3 altogether, making FHIR Release 4 the next de facto version the industry would move toward and coalesce behind.

Given FHIR Release 4's public release and that the industry will begin to implement Release 4 in parallel with this rulemaking, we request comment on the following options we could pursue for a final rule.

Option 1 (proposed in regulation text): Adopt just FHIR Release 2 for reference in proposed § 170.315(g)(10). This option would require health IT developers seeking certification to build, test, and certify systems solely to FHIR Release 2 and its associated implementation specifications. Under this option, if the National Coordinator approved the use of FHIR Release 3 or 4 (pursuant to the Standards Version Advancement Process) it would occur, at the earliest, one year after a final rule was issued. Given that timing, and the compliance deadlines proposed later in this section, it would mean that health IT developers would have no option but to develop to FHIR Release 2 in order to meet the proposed compliance deadlines.

Option 2: Adopt FHIR Release 2 and FHIR Release 3 in order to introduce optionality into how health IT developers are able to demonstrate compliance with proposed § 170.315(g)(10). In other words, by adopting and referencing both FHIR Release 2 and 3 in proposed § 170.315(g)(10) it would permit a health IT developer to use either one to meet the criterion (*i.e.,* both versions would not be required to be supported and demonstrating only one would be needed to meet certification). Similarly, under this option, if the National Coordinator approved the use of FHIR Release 4 (pursuant to the Standards Version Advancement Process) it would occur, at the earliest, one year after a final rule was issued. Given that timing, and the compliance deadlines proposed later in this section, it would mean that health IT developers would have no option but to develop to FHIR Release 2 or Release 3 in order to meet the proposed compliance deadlines.

Option 3: Adopt FHIR Release 2 and FHIR Release 4 in order to introduce flexibility into how health IT developers are able to demonstrate compliance with proposed § 170.315(g)(10). The full implementation of this option would depend on all applicable corresponding FHIR Release 2 implementation specifications also being published in their FHIR Release 4 formats and available prior to the issuance of a final rule. Provided these FHIR Release 4 implementation specifications are published in time for a final rule, this option would appear to be the best near- and long-term option for the industry. We anticipate this being the case because it would let lagging health IT developers catch up to the FHIR Release 2 baseline while at the same time enable leading health IT developers to move directly and immediately to FHIR Release 4 as a means to meet proposed

[81] In October 2018, ONC released a first version of a FHIR testing tool visit here for more details: *https://inferno.healthit.gov/.*

[82] *http://argonautwiki.hl7.org/index.php?title=Main_Page.*

[83] *https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/.*

[84] *http://blog.hl7.org/hl7-publishes-fhir-release-4.*

§ 170.315(g)(10)'s compliance timelines. In other words, unlike Options 1 and 2, the Standards Version Advancement Process would not be necessary and the trajectory of leading health IT developers would be well supported by the certification criterion. We also request comment on a variant of Option 3 that would include a pre-defined cut-over for the permitted use of and certification to FHIR Release 2. We note that if this variant were implemented as part of Option 3, we would likely also need to add a maintenance of certification requirement in the final rule to establish an upgrade timeline to FHIR Release 4 for those health IT developers who originally sought certification for FHIR Release 2. Such a maintenance requirement would seem necessary in order to bring the industry into closer alignment with respect to a more up-to-date national baseline for FHIR.

Option 4: Adopt solely FHIR Release 4 in the final rule for reference in proposed § 170.315(g)(10). This option would require health IT developers seeking certification to build, test, and certify systems solely to FHIR Release 4 and its associated implementation specifications. Again, provided all applicable FHIR Release 4 implementation specifications are published in time for a final rule, this option would appear to be a close preference to Option 3 for industry. We believe this would be the case because by the time a final rule associated with these proposals is issued, it is likely that health IT developers would have close to or over a year's worth of development experience with FHIR Release 4. As a result, many may be poised to introduce their first round of generally available FHIR Release 4 products into production. If ONC were to offer certification to FHIR Release 2 (as in Option 3) this flexibility could unintentionally delay the industry's transition to FHIR Release 4 and slow progress associated with FHIR-based interoperability. The following compliance timeline example attempts to make this point clearer. If, for example, the final rule was effective January 2020, based on other proposals associated with the API Conditions of Certification, health IT developers would have up to 2 years to rollout their (g)(10)–certified API technology, which would mean January 2022. At that point, FHIR Release 4 would have been published for nearly 3 years and FHIR Release 2 would have been published for nearly 6 years. Without a pre-defined cut-over for FHIR Release 2 in Option 3, that certification approach would permit FHIR Release 2 APIs to be deployed in 2022 and used for an indeterminate period of time.

In preparing your comments, please fully review our proposed certification criterion in § 170.315(g)(10) and the accompanying Conditions of Certification attributed to the API-oriented certification criteria. Notably, if we were to adopt another FHIR Release in a final rule as an alternative to FHIR Release 2 for the proposed API criterion in § 170.315(g)(10), then we would also adopt the applicable implementation specifications and FHIR profiles (the US FHIR Core profiles) associated with the FHIR Release in order to support USCDI data access. We highly encourage stakeholders to express their perspective and explicitly note their preferred option in comments.

ii. Proposed Adoption of Associated FHIR Release 2 Implementation Specifications

Our proposal to adopt the FHIR standard alone, however, is insufficient to provide the level of consistent implementation that will be necessary to realize the "without special effort" provision in this Condition of Certification. FHIR, much like other standards that are initially developed to be internationally applicable, requires additional implementation specifications in order to further constrain implementation choices and reflect US-based standards policies (such as the use of RxNorm for representing medications). In FHIR, the additional constraints placed on "base FHIR resources" are expressed through what are called "FHIR profiles." FHIR Profiles typically provide additional rules about which resource elements must be used and what additional elements have been added that are not part of the base FHIR resource. This can include, but not be limited to, rules about which API features are used and how as well as rules about which terminologies are used in particular elements. The term "profile" is a general term that is used in the FHIR standard to describe either an individual FHIR resource, or an entire implementation specification consisting of multiple FHIR resources. Accordingly, we propose to adopt three implementation specifications that will establish a standardized baseline and further constrain API conformance to help assure that APIs can be used "without special effort."

We propose to adopt in § 170.215(a)(2) an implementation specification that would list a set of base FHIR resources that Health IT Modules certified to the proposed criterion in § 170.315(g)(10) would need to support. We refer to this proposed initial set of FHIR resources as the "API Resource Collection in Health" or "the ARCH." The ARCH would align with and be directed by the data policy specified in the proposed US Core Data for Interoperability (USCDI) standard (discussed in section IV.B.1 of this proposed rule).

As a result, we propose to include 15 FHIR resources in the ARCH's first version. Based on prior industry efforts, including the Argonaut Project to map FHIR resources to the previously defined Common Clinical Data Set (CCDS), we know that the following 13 FHIR resources map to and support the equivalent data classes specified in the USCDI: AllergyIntolerance; CarePlan; Condition; Device; DiagnosticReport; Goal; Immunization; Medication; MedicationOrder; MedicationStatement; Observation; Patient; and Procedure. We also propose to include, specifically for the Patient resource that the "Patient.address" and "Patient.telecom" elements must be supported as part of the Patient resource. These elements are neither required in the base FHIR resource or additional implementation specifications; however, they are necessary to align with the USCDI's data requirements. With respect to the Device resource, we propose to require that the "Device.udi" element follow the human readable representation of the unique device identifier (UDI) found in the recommendation, guidance, and conformance requirements section of the "HL7 Version 3 Cross Paradigm Implementation Guide: Medical Devices and Unique Device Identification (UDI) Pattern, Release 1," a document hosted by HL7.[85] Developers would be held responsible only for the recommendation, guidance, and conformance requirements for HL7 FHIR in the implementation guide and would not be held responsible for other requirements in the implementation guide specific to other standards, including requirements for HL7 Version 2 and HL7 Version 3. For clarity, these proposed requirements are part of the ARCH Version 1 standard.

In addition to these 13 FHIR resources, we have included two additional FHIR resources:

(1) The Provenance resource; and (2) the DocumentReference resource to accommodate clinical notes. These additions would make for a total of 15 FHIR resources to reflect the direction of the USCDI v1. With respect to clinical notes, we understand from our own

[85] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=487.*

analysis and technical discussions within HL7 that the FHIR DocumentReference resource is best capable of handling the exchange of clinical notes. Since the CCDS was defined over two years ago, we have most frequently heard from provider stakeholders that access to ''clinical notes'' is key, impactful, and highly desirable data that should be accessible via the C–CDAs they exchange as well as via APIs. While we realize the industry may need to develop additional implementation guidance to support clinical notes via FHIR, we believe that including FHIR resources in ARCH Version 1 directly addresses the steady requests we have received from providers to include a focus on the access, exchange, and use of ''clinical notes'' as part of certification. Thus, we propose to include the FHIR DocumentReference resource in the ARCH to support clinical notes. We also clarify that the clinical note text included in this FHIR resource would need to be represented in its ''raw'' text form. In other words, it would be unacceptable for the note text to be converted to another file or format (*e.g.,* .docx, PDF) when it is provided as part of an API response. With respect to the Provenance resource, we believe its inclusion in the ARCH is paramount to the long-term success and use of FHIR-based APIs. While C–CDA's are often critiqued due to their relative ''length,'' the C–CDA often represents the output of a clinical event and includes relevant context. The same will not always be true in an API-context. This is due to the fact that FHIR-based APIs make it significantly easier for apps to request specific data (*e.g.,* just a patient's active medications). Thus, it is equally important over the long-term that the industry not lose sight of the metadata (*i.e.,* the who, what, when, where, why, and how) behind the data that was created. As a result, we believe that this early stage of FHIR deployment is the best time for the industry to build in support for the Provenance resource. Otherwise, if we were to expand the ARCH in future years to include this FHIR resource, we estimate that the developer burden and overall industry impact would be greater than building this support in ''from the start.'' Specifically, and to remain consistent with the USCDI, we propose to require that the ''Provenance.recorded'' (for the author's time stamp) and ''Provenance.agent.actor'' (for the author and author's organization) elements be supported as part of the Provenance resource.

Over time, and as the USCDI is expanded, we also expect to update this implementation specification to expand the ARCH beyond these 15 FHIR resources. Equally, consistent with the Maintenance of Certification requirements described in section VII.B.5 of this proposed rule (the Standards Version Advancement Process proposals), which would permit health IT developers to voluntarily implement and use a new version of an adopted standard or implementation specification so long as certain conditions are met including that the new version is approved by the National Coordinator for use in certification through the Standards Version Advancement Process, health IT developers would be able to update their certified health IT to include (g)(10)-certified API access to a broader set of data once a new version of the ARCH is approved.

The next implementation specification for the FHIR standard we propose to adopt in § 170.215(a)(3) is the Argonaut Data Query Implementation Guide version 1 (Argonaut IG), hosted by HL7.[86] This implementation guide has been pilot tested and is now being implemented for production use by health IT developers. Notably, it specifies FHIR profile constraints for 13 of the associated FHIR resources we propose to include in the ARCH Version 1 and these FHIR profiles support the data included in the USCDI (v1).

The next implementation specification for the FHIR standard we propose the Secretary adopt in § 170.215(a)(4) is the specific portion of the Argonaut IG that refers to the ''Argonaut Data Query Implementation Guide Server'' conformance requirements. While it could be implied through our proposed adoption of the Argonaut IG that these conformance requirements would be included, we seek to make this an explicit requirement for the API certification criterion proposed in § 170.315(g)(10). Conformance to this implementation specification is essential in order to ensure that all FHIR servers are consistently configured to support the defined data queries and ''supported searches'' associated with each Argonaut profiled FHIR resource. For clarity, conformance testing would focus on and be limited to the ''SHALL'' requirements. We also note that the Argonaut Data Query Implementation Guide Server includes conformance requirements for the ''DocumentReference Profile,'' which defines ''how a provider or patient can retrieve a patient's existing clinical document.'' This particular specification was produced in support of the 2015 Edition certification criterion adopted in § 170.315(g)(9). As a result, we clarify that this specific portion of the Server IG and conformance requirement would be out of scope for the purposes of proposed § 170.315(g)(10).

We have separately proposed the FHIR standard and each of these implementation specifications so that the National Coordinator may evaluate industry progress and make a unique or combined determination as to the appropriate time to approve for voluntary upgrade pursuant to the standards version advancement process discussed in more detail in section VII.B.5 as well as subsequently go through rulemaking to adopt a new version of: The FHIR standard, the ARCH, implementation specifications that ''profile'' the resources in the ARCH, and implementation specifications for FHIR server conformance capabilities. While the proposed implementation specifications relate to one another, they can also be updated independently of each other as time goes on. For instance, the National Coordinator could approve a new version of the FHIR standard ''Release 5'' in the future in accordance with the standards version advancement process. In so doing, the National Coordinator could leave the scope of the ARCH the same and update (necessarily) the implementation specifications for the FHIR profiles and FHIR server conformance requirements accordingly to align with the new FHIR version. As an alternative example, the National Coordinator could leave the FHIR standard version the same and approve a new version of the ARCH to include more FHIR resources.

We note that other federal agencies may be adopting the FHIR standard and additional FHIR implementation guides for their program requirements. We plan to coordinate with such other agencies to focus on strategic alignment among the FHIR standard versions, applicable implementation guides, and use cases.

iii. Proposed Adoption of Standards and Implementation Specifications To Support Persistent User Authentication and App Authorization

To enable and support persistent user authentication and app authorization processes, we propose to adopt a standards and additional implementation specification for the FHIR standard. First, we propose to adopt the ''OpenID Connect Core 1.0

[86] *http://www.fhir.org/guides/argonaut/r2/.*

incorporating errata set 1'' standard in § 170.215(b) as it complements the SMART Application Launch Framework Implementation Guide Release 1.0.0[87] (SMART Guide). The OpenID standard is typically paired with OAuth 2.0 implementations and focuses on user authentication. Second, we propose to adopt the SMART Guide in § 170.215(a)(5) as an additional implementation specification associated with the FHIR standard. This guide is referenced by the Argonaut IG and is generally being implemented by the health IT community as a security layer with which FHIR deployment is being combined (from both a FHIR server and FHIR application perspective). Further, while the SMART Guide includes certain mandatory requirements, we believe three specific aspects are necessary to specifically require in order for certification to enable consistent industry-wide implementation.

The SMART Guide specifies the use of ''refresh tokens'' as optional. We believe that this requirement is necessary in order to enable persistent access by apps, especially in a patient access context. Thus, we propose to make their use mandatory with a minimum refresh token life of 3 months. While this technique would need to be supported for both types of API-enabled services we propose be supported through § 170.315(g)(10), we wish to emphasize that implementing refresh token support is directly intended to enable a patient's ''persistent access'' to their electronic health information without special effort (*i.e.,* without having to frequently re-authenticate and re-authorize while using their preferred app). This proposal aligns with the industry developed security best practice guidelines for OAuth 2.0 implementations, which require support for a short-lived ''access token'' and a long-lived ''refresh token'' that could be subsequently used by the app to obtain a new ''access token'' after the original ''access token'' expires. We believe this approach enhances the seamlessness of a patient's data access and reduces the ''friction'' they would otherwise experience having to re-authenticate and re-authorize. At the same time, because the access token is short lived, this minimizes the risk of a patient's information being accessed by unauthorized users if for some reason the access token is compromised. The technical capabilities that we intend to explicitly test are referenced as part of the proposed API certification criterion in § 170.315(g)(10).

We also propose to require that the ''Standalone Launch'' and ''EHR Launch'' requirements specified in the SMART Guide be supported. We believe that requiring API Technology Suppliers to demonstrate both of these capacities will help ensure greater standardization and ease of use among (g)(10)-certified APIs. When a third-party ''app'' first connects to a FHIR server, it often requires some contextual data to make the app more ''user friendly.'' This information could include things such as the most recent patient encounter or hospital visit. The contextual information depends on how the ''app'' is launched.

When an app is launched from ''outside of an EHR,'' such as from a patient's smartphone or web browser, then the app is considered to be launched in a ''Standalone'' mode. In this mode, the app has to request that the FHIR server provide appropriate contextual information, which can then be used to customize the app's display for the patient. The SMART Guide has standardized the information that such apps can request from FHIR servers and defined it as ''Standalone Launch.''

In other contexts, apps can be launched from ''within the EHR.'' This is typically the case when a third-party app is integrated as part of an EHR technology. In this case, the app is considered to have been launched in the ''EHR'' mode. Typically, when such an app is launched from within an EHR, the user (*e.g.,* provider, nurse) has a patient's record ''open'' or ''active'' in the EHR and expects the app to directly open the same patient when it is launched. In order for this to happen, the app has to request that the FHIR server provides information about the patient record that is currently ''open'' in the EHR. The SMART Guide has standardized this interaction and defined it as ''EHR Launch.''

iv. Proposed Adoption of a New API Certification Criterion in § 170.315(g)(10)

Proposal Overview

To implement the Cures Act, we propose to adopt a new criterion in § 170.315(g)(10) to replace the certification criterion adopted in § 170.315(g)(8). Currently, the criterion adopted in § 170.315(g)(8) focuses on a Health IT Module's ability to provide API functionality that can respond with data for each of the data categories specified in the Common Clinical Data Set. Moreover, its focus on read-access/response to requests for specific types of data most directly aligns with the API uses envisioned by industry stakeholders and the Cures Act, which is why we believe it is necessary and appropriate to replace § 170.315(g)(8). In contrast, we do not propose that it is necessary to replace the certification criteria adopted in § 170.315(g)(7) and (g)(9) because the former does not prescribe specific technical approaches (and can continue to be met as technology evolves) and the latter supports a discrete use case relative to an API function that responds with a C–CDA.

We propose our approach to adopt a replacement for § 170.315(g)(8) that will provide clear regulatory compliance requirements for stakeholders because: (1) 2015 Edition testing and certification to § 170.315(g)(8) will continue throughout this rulemaking; (2) presuming we adopt this (or a modified version of this) proposal in a final rule, it will be easier for the industry to distinguish compliance requirements between two separate certification criteria compared to a time/context-sensitive ''version'' of § 170.315(g)(8); and (3) § 170.315(g)(8) is currently specified in the Base EHR definition so its replacement has compliance effects on health care providers participating in every program that requires the use of Certified EHR Technology, which references the Base EHR definition.

At a high-level, we propose that this new API certification criterion would require FHIR servers to support two types of API-enabled services:

- Services for which a single patient's[88] data is at focus; and
- services for which multiple patients' data are at focus, which, hereafter, we refer to as ''population-level'' to convey the grouped and cohort scope on which the data associated with these services would be focused (*e.g.,* a specific provider's patient panel, all of the patients covered by a particular health plan, a group of patients cared for through an alternative payment model).

This proposed certification criterion would only require mandatory support for ''read'' access for both identified services, though we envision a future version of this certification criterion that could include specific ''write'' conformance requirements (for example, to aid decision support) once FHIR-based APIs are widely adopted. In all cases, this proposed criterion will require that the two types of API services have appropriate security controls implemented. These controls

[87] *https://build.fhir.org/ig/HL7/smart-app-launch/.*

[88] We recognize that individuals may not always be in an active role as a ''patient'' when they use an application to access their data. However, we believe it is clearer for the purposes of readability and policy intent to use the term ''patient'' as opposed to ''individual.''

would ensure a user fully authenticates to the API-enabled data source to which the request is being made and that the user's software application is appropriately authorized to request specified data.

API services that focus on a single patient would include, but not be limited to, those that interact with software applications controlled and used by a patient to access their data as well as software applications implemented by a provider to enhance their own ''internal'' clinical care tools and workflow (*e.g.,* a specialized calculation app). Most, if not all, of these types of interactions are typically orchestrated in a synchronous, real to near-real-time mode via APIs.

Conversely, API services that focus on multiple patients would include, but not be limited to, software applications used by a health care provider to manage various internal patient populations as well as external services a health care provider may contract for to support quality improvement, population health management, and cost accountability vis-à-vis the provider's partners (*e.g.,* health plans). Historically, access to this kind of computing has often been cumbersome, opaque, and required one-off scripting and significant engineering labor with no overarching standardized methods. By shifting this paradigm to a FHIR-based API, we anticipate that the market will be able to respond with a new slate of innovative solutions.

Across this spectrum of population-level uses, the scope or quantity of the data may range from a small group to many hundreds or thousands of patients. Moreover, when ''external'' applications and services are provided access to patient data by the provider, we expect that such access and associated privacy and security protocols would be established consistent with existing legal requirements under the HIPAA Privacy and Security Rules (including business associate agreements), other data use agreements (as applicable), and any other state or federal applicable law. Principally, for the purposes of the proposed certification criterion, we seek to include and ensure through testing and certification that a set of baseline API functionality exists and is deployed for providers to use at their discretion to support their own clinical priorities as well as to use to engage with their partners, such as software developers and developers of third-party applications.

We have explicitly proposed to include support for API services that are population-level focused in this certification criterion because the current certification criterion in § 170.315(g)(8) has largely been tested, certified, and deployed to support the ''patient data request'' use case. In comparison, population-level focused API services are envisioned to support FHIR-based apps that not only improve clinical workflow and decision support but also help advance a learning health system. In so doing, providers, payers, and other stakeholders will be able to make incrementally better use of FHIR's RESTful API and JSON payload to apply modern computing techniques, including big data analyses and machine learning, to account for, assess, and inform the quality and effectiveness of care delivered. As noted in the proposed API standards section, FHIR Release 4 includes technical specifications to enable standardized population-level services via FHIR-based APIs in a more efficient manner than currently possible. If ''Option 3'' or ''Option 4'' is preferred by industry in terms of the FHIR standards options for this certification criterion, these approaches would be demonstrable. Alternatively, if the National Coordinator were to approve FHIR Release 4 for use under this proposed certification criterion (following the Standards Version Advancement Process described in Section VII.B.5 of this preamble) then it would be able to be used to meet these technical expectations.

Lastly, as we considered the necessary oversight responsibilities the Cures Act adds to the Program, we have determined that it would be essential to include a specific population-level API conformance requirement as part of this criterion so that such capabilities could be evaluated post-certification for compliance with (among other requirements) this API Condition of Certification and the information blocking and real world testing Conditions of Certification.

Specific Proposals

In general, we have approached framing § 170.315(g)(10) in the same way we framed § 170.315(g)(8). This new proposed criterion, however, includes some important differences and specificity compared to § 170.315(g)(8). Taken together, the following proposals are designed to establish a consistent set of API implementation requirements aimed at the API Condition of Certification's ''without special effort'' requirement. We propose that API technology presented by a health IT developer (otherwise considered an API Technology Supplier in this context) for testing and certification to the proposed certification criterion in § 170.315(g)(10) would need to meet the requirements outlined below. We seek comment on all of the following proposals.

Data Response

We propose in § 170.315(g)(10)(i) that the health IT presented for testing and certification must be capable of responding to requests for data on a single patient and multiple patients associated with each of the FHIR resources specified in ARCH Version 1 and consistent with FHIR Release 2 and the Argonaut IG implementation specification. More specifically, we clarify that all data elements indicated as ''mandatory'' and ''must support'' by the proposed standards and implementation specifications must be supported and would be in scope for testing. Through this approach, certification will provide for a consistent and predictable starting scope of data from which apps and other services can be developed.

Search Support

We propose to require in § 170.315(g)(10)(ii) that the health IT presented for testing and certification must be capable of responding to all of the ''supported searches'' specified in the Argonaut Data Query Implementation Guide Server, which as a reminder we have proposed for adoption as an implementation specification in § 170.215(a)(4).[89] Given that there is not yet a consistent, standardized specification for FHIR servers to handle searches for multiple patients, we clarify that a health IT developer would be permitted to approach searches for multiple patients in the manner it deems most efficient to meet this proposed certification criterion. We note, consistent with the implementation specifications current scope, that conformance would focus on search associated with a single patient's data. However, we reiterate the health IT presented for testing and certification and as implemented must support searches for multiple patients independent of a required standard for such searches.

For the DocumentReference and Provenance resources, which are currently present in the base FHIR standard, we request comments on the minimum ''search'' parameters that would need to be supported.

[89] *http://www.fhir.org/guides/argonaut/r2/Conformance-server.html.*

App Registration

We propose in § 170.315(g)(10)(iii) that health IT presented for testing and certification must be capable of enabling apps to register with an ''authorization server.'' This proposed conformance requirement would require an API Technology Supplier to demonstrate its registration process, but would not require that it be done according to a specific standard. We considered proposing the OAuth 2.0 Dynamic Client Registration Protocol (*RFC 7591*) standard (''Dynamic Registration'') as the only way to support registration for this certification criterion and request public comment on whether we should require its support as part of a final rule's certification criterion. For clarity, we note that while we have not explicitly required Dynamic Registration as the only way to demonstrate conformance with this specific portion of the certification criterion, API Technology Suppliers would still be allowed to use Dynamic Registration if they so choose.

While requiring Dynamic Registration could create a more consistent registration experience for health IT developers, we did not expressly include this standard because of its relatively low adoption and implementation in the health IT ecosystem. Notably, while the SMART Guide covers a majority of technical steps necessary for an app to connect a FHIR server, it is neutral on the registration process API Technology Suppliers could take. Much like we did with § 170.315(g)(8) in the initial 2015 Edition final rule by not requiring FHIR, we believe that a prudent approach for registration is to require that it be addressed from a functional perspective while the industry reaches consensus on the best techniques to enable registration.

Note, that while this portion of proposed § 170.315(g)(10) focuses on the technical standards conformance, we have also included a specific ''maintenance requirement'' associated with the API Condition of Certification around the timeliness of this registration process in production settings as applicable to API Technology Suppliers. This proposed requirement will ensure that patients are able to use their apps in a timely manner.

We do not intend to test registration capabilities for apps that would be executed within an API Data Provider's clinical environment. We believe this discretion is warranted as API Technology Suppliers and API Data Providers are best poised to innovate and execute various methods for app registration within a clinical environment. However, we request comment on this perspective.

Secure Connection, Authentication and Authorization

We propose in § 170.315(g)(10)(iv) that the health IT presented for testing and certification must be capable of establishing a secure and trusted connection with an application that requests patient data in accordance with the SMART Guide. In the context of this proposed criterion, this would require that an ''authorization server'' be deployed and support, at a minimum, ''authorize'' and ''token'' endpoints and the publication of the endpoint URLs via FHIR server's metadata as specified in the SMART Guide to enable automated discovery by apps. Again, we note, consistent with this implementation specification's current scope, that initial conformance would focus on the secure connection parameters with a single patient's data in mind. Given that there is not yet a consistent, standardized specification for FHIR servers to handle secure connection parameters for multiple patients, we clarify that a health IT developer would be permitted to approach secure connections for multiple patients in the manner it deems most efficient to meet this proposed certification criterion.

When an application connects to request data for the first time, we propose in § 170.315(g)(10)(v)(A) that health IT presented for testing and certification must be capable of demonstrating support for user authentication according to the OpenID Connect Core 1.0 incorporating errata set 1 [90] standard. It should be noted that the OpenID Connect Standard is agnostic to the actual authentication mechanism used by the health IT while providing a standard way for health IT to exchange the authentication information to the app. The primary benefit being that it lets apps verify the identity of the end-user based on the authentication performed by the Authorization Server without having the apps to take additional responsibility for authenticating the user. We also propose in § 170.315(g)(10)(v)(B) that health IT presented for testing and certification must demonstrate that users can authorize applications (in the appropriate context) to access data in accordance with the SMART Guide. Pursuant to this proposed implementation specification described above, we also intend to test health IT in the ''Standalone Launch'' and ''EHR Launch'' modes. Additionally, we clarify that for the purposes of testing and certification, we propose to require that health IT support only a limited set of capabilities related to the OpenID Connect Standard—specifically, only those that are specified in the SMART Guide.

Further, in order to enable patients and providers to get persistent access to health information without having to re-authenticate and re-authorize, we propose to require that a ''refresh token'' must be provided with an expiration period of at least 3 months from the date issued. The ''refresh token'' could be subsequently used by the app to obtain a new ''access token'' after the expiration of the original ''access token.'' Note the proposed refresh token requirement is different than providing an ''access token'' with an extended life, which is typically discouraged from a security best practice perspective so as to prevent unauthorized access if for some reason the access token were to be acquired for use by an unauthorized application.

We propose in § 170.315(g)(10)(vi) that health IT presented for testing and certification must demonstrate that it can support subsequent connections by an app and requests data without requiring the user to re-authorize and re-authenticate when a valid refresh token is supplied. Further, we propose that once a valid refresh token has been used to get a new access token that the FHIR server must demonstrate that it can issue a new refresh token to the app, which must be for a new period no shorter than three months. For example, if an application were issued a refresh token that was good for three months upon its first-ever connection and then subsequently connected to the FHIR server one month later, the FHIR server would need to enable that connection to occur without re-authentication and re-authorization, and it would need to issue a new refresh token for a new three-month period from that access date. Again, we intend to test health IT in the ''Standalone Launch'' and ''EHR Launch'' contexts pursuant to the SMART Guide.

We have proposed this renewal requirement because industry stakeholders at various meetings and conferences at which we have attended have indicated that a constant need for patients to re-authenticate and re-authorize their apps creates usability challenges and may otherwise contradict the Cures Act's intent associated with the phrase ''without special effort.'' Further, we are not aware of a standard, consistent

[90] *http://openid.net/specs/openid-connect-core-1_0.html.*

methodology for specifying the lifetime of refresh tokens in published technical specifications. As a result, we believe our approach would improve the current user experience for patients and providers alike. Additionally, authorization servers maintain binding between the refresh token and the application to whom it was issued, and hence can protect against misuse by unauthorized applications.

We believe that the three-month period is a reasonable length given the proposal for the re-issuance of a new refresh token. However, we acknowledge that this same policy outcome we discuss above could be achieved by, for example, having a two-month period. Accordingly, we seek comment on whether there are available specifications we should review as well as whether there should be a reasonable upper bound from a timing perspective (*e.g.,* one year) after which the user should be required to re-authenticate and re-authorize.

For both the first time connection and subsequent connection proposals, we recognize that there is not yet a consistent, standardized specification for FHIR servers to handle data requests for multiple patients. As noted above, we expect that FHIR Release 4 will have such specificity. However, for the purposes of meeting this proposed certification criterion, we clarify that a health IT developer would be permitted to approach requests for multiple patients in the manner it deems most efficient.

Transparency Through the Publication of API Documentation

In the 2015 Edition final rule we included transparent documentation requirements for all three of the API-focused certification criteria adopted in § 170.315(g)(7) through (g)(9). These requirements specified that documentation associated with API syntax (and other technical descriptors), the software components and configurations that would be necessary in order for a deployed API to successfully work, and the terms of use for the API be made publicly available. We continue to believe that such a requirement is important for proposed § 170.315(g)(10), especially in light of the Cures Act's ''without special effort'' provision. Such transparency and openness is commonplace in many other industries and has fueled innovation, growth, and competition. Further, we believe that full transparency is necessary to ensure that software developers building to a health IT developer's (g)(10)-certified API have a thorough understanding of any requirements against which their software will need to be designed.

In reconciling the 2015 Edition final rule's API documentation requirements with the new expectations set forth by the Cures Act regarding a health IT developer's practices, we have determined that revisions are necessary. Accordingly, we propose to revise the documentation provision in the API certification criteria adopted in § 170.315(g)(7) through (g)(9) as well as reflect the same revision in proposed § 170.315(g)(10) and (11). Specifically, we propose to focus the documentation requirement set forth by the certification criteria on solely the technical documentation associated with the API technology. As a result, we propose to remove the provision in § 170.315(g)(7) through (g)(9) associated with ''terms of use'' as this type of documentation could be considered more reflective of business practice and better placed with other similar requirements. Consistent with the Cures Act's API Condition of Certification, we have proposed more detailed Condition of Certification requirements associated with a health IT developer's API terms of use in order to address business practices that could interfere with and create special effort on the part of an API User.

With respect to the technical documentation that would need to be made publicly available, we recognize that our proposed formal adoption of the FHIR standard and the associated implementation specifications (for § 170.315(g)(10)) would be consistent across all health IT presented for certification. As a result there may be minimal additional documentation needed for these capabilities beyond what is already documented in these standards and specifications. However, pursuant to the limited mandatory scope proposed for ''data response'' (for § 170.315(g)(10)), we believe that API Technology Suppliers should disclose any additional data their (g)(10)-certified API supports in the context of FHIR resources referenced in ARCH Version1 and associated implementation specifications. For example, the Argonaut IG ''Patient Profile'' includes optional elements for marital status, photo, and contact (as in contact person like a guardian or friend). To the degree that a (g)(10)-certified API supports such optional data an API Technology Supplier would be required to convey this support in its published technical documentation. Additionally, we note that other specifications, like the RFC 7591, provide developers some latitude in terms of the information that could be supplied for the purposes of registration.

Thus, we propose in § 170.315(g)(10)(vii) that an API Technology Supplier would need to provide detailed information for all aspects of its (g)(10)-certified API, especially for any unique technical requirements and configurations, such as how the FHIR server handles requests for multiple patients (until such time as there is an approved standardized approach that can be cited) as well as app registration requirements. For aspects that are not unique and are fully specified by the FHIR standard and associated implementation specifications, the developer could include hyperlinks to this information as part of its overall documentation. Further, we propose to include the word ''complete'' in the documentation provision in order to make this point explicit and link this obligation to the associated transparency conditions proposed as part of the overall Condition of Certification. We note for health IT developers that the documentation published must be of the sort and to the level of specificity, precision, and detail that the health IT developer customarily provides to its own employees, contractors, and/or partners who develop software applications for production environments.

Lastly, we note that all of the documentation referenced by this criterion must be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, ''click-through'' agreements, or requirement to provide contact details or other information prior to accessing the documentation. It would also require that such documentation needs to be submitted as part of testing for this certification criterion and subsequently to ONC–ACBs for review prior to issuing a certification.

d. Condition of Certification Requirements

To implement the Cures Act, we have designed this API Condition of Certification in a manner that will complement the technical capabilities described in our other proposals, while addressing the broader technology and business landscape in which these API capabilities will be deployed and used.

Consistent with the attributes we have identified for the statutory phrase ''without special effort,'' our overarching vision for this Condition of Certification is to ensure that (g)(10)-certified APIs, among all API technology, are deployed in a manner that supports an experience that is as seamless and frictionless as possible. To that end, we seek to promote a standards-based ecosystem that is transparent, scalable, and open to robust competition and innovation.

The specific requirements of this Condition of Certification are discussed in several sections below. These requirements would address certain implementation, maintenance, and business practices for which clear and consistent parameters are needed to ensure that API technology is deployed in a manner that achieves the policy goals we have described. The proposed requirements would also align this Condition of Certification with other requirements and policies of the Cures Act that promote interoperability and deter information blocking, as discussed in more detail in the sections that follow.

i. Scope and Compliance

To start this Condition of Certification, we propose in § 170.404 to apply this Condition of Certification to health IT developers with health IT certified to any of the API-focused certification criteria. These criteria include the proposed ''standardized API for patient and population services'' (§ 170.315(g)(10)) and ''consent management for APIs'' (§ 170.315(g)(11)) as well as the current ''application access—patient selection'' (§ 170.315(g)(7)), ''application access—data category request'' (§ 170.315(g)(8)), ''application access—all data request'' (§ 170.315(g)(9)). In other words, this entire Condition of Certification would not apply to health IT developers that do not have technology certified to any of these API-focused certification criteria. Similarly, this condition is solely applicable to these API-focused certification criteria. As a result, the proposed policies for this Condition of Certification would not apply to a health IT developer's practices associated with, for example, the immunization reporting certification criterion adopted in § 170.315(f)(1) because that criterion is not one of the API-focused criteria. However, health IT developers should remain mindful that other proposals in this proposed rule, especially those related to information blocking, could still apply to its practices associated with non-API-focused certification criteria.

Given the proposed applicability of this condition to current API-focused criteria and that health IT developers with products certified to §§ 170.315(g)(7)–(9) would need to meet new compliance requirements associated with such criteria, we also propose certain compliance timelines associated with this Condition of Certification that would need to be met.

ii. Cures Act Condition and Interpretation of Access to ''All Data Elements''

First, we propose to adopt the Cures Act's API Condition of Certification in § 170.404(a)(1) to fully incorporate the statute's compliance requirements. Second, strictly for the scope of the API Condition of Certification, we propose to interpret the meaning of the phrase ''all data elements of a patient's electronic health record'' as follows.

For the reasons discussed above, the proposed § 170.315(g)(10) certification criterion and associated standards and implementation specifications would facilitate API access to a limited set of data elements (*i.e.,* from the FHIR resources that ARCH Version 1). Accordingly, for the purposes of meeting this portion of the Cures Act's API Condition of Certification, we interpret the scope of: The ARCH; its associated implementation specifications; and the policy expressed around the data elements that must be supported by (g)(10)-certified APIs (*i.e.,* FHIR servers) to constitute ''all data elements.'' Given other proposals related to permitting the use of updated versions of adopted standards and implementation specifications, we expect that (g)(10)-certified APIs will be able to support access to more data over time in response to updates to the USCDI and the ARCH. As these updates occur, the industry would be able to incrementally approach the totality of data that can be electronically accessed, exchanged, and used pursuant to the Cures Act's reference to ''all data elements.''

Again, we reiterate that this specific interpretation does not extend beyond the API Condition of Certification and cannot be inferred to reduce the scope or applicability of other Cures Act Conditions of Certification or the information blocking proposals, which necessarily will include a larger scope of data. For example, other Conditions of Certification will apply to health IT developer behaviors associated with data that are not part of the USCDI or ARCH, such as the proposals at 45 CFR 170.402 and the proposals in Part 171, which apply across several stakeholders including health information networks and health care providers.

iii. Transparency Conditions

We propose as part of this Condition of Certification that API Technology Suppliers be required to make specific business and technical documentation freely and publicly accessible. Thus, we propose to adopt several transparency conditions as part of § 170.404(a)(2).

Similar to our policy associated with the API-focused certification criteria, we propose in § 170.404(a)(2)(i) that all published documentation be complete and available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. For example, the API Technology Supplier cannot impose any access requirements, including, without limitation, any form of registration, account creation, ''click-through'' agreements, or requirement to provide contact details or other information prior to accessing the documentation.

Terms and Conditions Transparency

In addition to technical documentation, we propose in § 170.404(a)(2)(ii)(A) to require API Technology Suppliers to publish all terms and conditions for use of its API technology. We believe that it is important to make this information readily accessible to API Data Providers, API Users, app developers, and other persons. This transparency would ensure that these stakeholders do not experience ''special effort'' in the form of unnecessary costs or delays to obtain the terms and conditions for API technology. Further, we believe that full transparency is necessary to ensure that app developers have a thorough understanding in advance of any terms or conditions that might apply to them and do not encounter unanticipated hurdles once they have committed to developing software or attempt to implement or deploy such software in production.

We note that this requirement would apply to *all* terms and conditions that apply to the API technology and its use. As noted above, and for the purposes of this proposal's scope, ''API technology'' refers to the specified API capabilities for Health IT Modules certified to § 170.315(g)(7) through (11) under the Program. We consider ''terms and conditions'' to include any fees, restrictions, limitations, obligations, registration process requirements, and other terms or conditions that would be material and needed to:

- Develop software applications to interact with the API technology;
- distribute, deploy, and enable the use of software applications in production environments that use the API technology;
- use software applications, including to access, exchange, and use EHI by means of the API technology;

- use any EHI obtained by means of the API technology; and
- register software applications (as discussed in more below).

In addition, we propose in § 170.404(a)(2)(ii)(B) that any and all permitted fees charged by an API Technology Supplier for the use of its API technology must be published and described in detailed, plain language as part of its publicly available terms and conditions. The description of the fees must include all material information, including, but not limited to, the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

For the purposes of the specific transparency conditions proposed in § 170.404(a)(2) and their relationship and applicability to API Technology Suppliers with products already certified to § 170.315(g)(7), (8), or (9), we propose to establish a compliance date of six months from the final rule's effective date (which would give developers approximately eight months from the final rule's publication date) to revise their existing API documentation to come into compliance with the final rule. We also recognize that API Technology Suppliers will need to update the proposed publicly available information from time to time. Thus, for the purposes of and with respect to subsequent updates to this information, we expect API technology suppliers to make clear to the public the timing information applicable to their disclosures (*e.g.,* effective/as of date or last updated date) in order to prevent out of sync discrepancies in what an API Technology Supplier's public documentation states and what it may be communicating directly to its customers (*e.g.,* a change in fees is directly communicated to customers but not reflected at the publicly available hyperlink pursuant to its responsibilities under this proposal). If an API Technology Supplier's actions are out of sync with its publicly provided documentation, the API Technology Supplier would be at risk of violating this Condition of Certification. We request public comment on whether this expectation should be formally specified in regulation text or if these ''effective date'' approaches for changes to transparency documentation are common place such that it would be a standard practice as part of making this documentation available.

We also note that API Technology Suppliers would be expected to revise and/or construct terms and conditions for its API technology that account for and reflect the proposals associated with this API Condition of Certification and information blocking policies. In so far as an API Technology Supplier would find it necessary to enforce its published terms and conditions, we caution API Technology Suppliers to be mindful of whether such terms and conditions would be acceptable and consistent with the aforementioned policies in the first place—as an impermissible term or condition would be problematic regardless of whether it was actively enforced.

We propose in § 170.404(a)(2)(ii)(C) a final transparency condition associated with API Technology Suppliers' application developer verification processes that takes into account the fact that we did not propose to adopt the Dynamic Registration standard as part of proposed § 170.315(g)(10). Had we proposed requiring Dynamic Registration, we would have also proposed a specific Condition of Certification that would have outright prohibited API Technology Suppliers from identity proofing or verifying authenticity of an app developer when it came to apps that were designed to enable patient access.

On balance, however, we believe that permitting API Technology Suppliers to institute a process to verify the authenticity of application developers will foster additional trust in the growing API ecosystem. We seek comments and recommendations on factors that would enable registration with minimal barriers. For example, permitting API Technology Suppliers to do one- time verification of the app developers (or even rely on centralized vetting by a trusted third party), which would allow the developer's future apps to automatically register without case- by- case checks (or checks for each API Technology Supplier with which the app developer interacts). One risk to consider with Dynamic Registration plus a prohibition on vetting, for instance, is that it would be much easier for a malicious app developer to spoof another legitimate app developer's app. Such an action could ultimately lead to confusion and distrust in the market. However, the Dynamic Registration option would minimize barriers to registration especially for third-party apps designed to enable patient access. We seek comments on options and trade-offs we should consider.

Accordingly, and weighing those concerns with the Cures Act's ''without special effort'' provision and our proposed information blocking policies, we specifically propose to permit API Technology Suppliers to institute a process to verify the authenticity of application developers so long as such process is completed within five business days[91] of receipt of an application developer's request to register their software application with the API technology's authorization server. To clarify, this verification process would need to focus specifically on the application developer—not its software application(s). We also clarify that API Technology Suppliers would have the discretion to establish their verification process so long as the process is objective and the same for all application developers and it can reasonably be completed within the five business days—otherwise such a process could risk implicating/violating other elements of this proposed API Condition of Certification as well as information blocking behaviors. The following includes a few non-exhaustive examples of verification techniques that could be used by an API Technology Supplier to have additional certainty about the application developer with whom they are interacting: Instituting a ''penny verification'' process, requiring some form of corporate documentation, or requesting other forms of authenticating documentation or transactions.

We believe that five business days is sufficient time for API Technology Suppliers to weed out malicious developers seeking to deceive the API Technology Supplier, API Data Providers or API Users, but request public comment on other timing considerations. Moreover, we clarify that this proposed Condition of Certification is meant to set the upper bound for a verification process an API Technology Supplier would be permitted to take and should not be interpreted as compelling API Technology Suppliers to institute such a process (*i.e.,* API Technology Suppliers would not be required to institute a verification process). Rather, for those API Technology Suppliers that see it in their (as well as their customers and patients) best interests to institute such a process, we have laid out the rules that we believe meet the Cures Act's without special effort expectations. If an API Technology Supplier chooses not to institute an app developer verification process prior to enabling the production use of an app, it would solely need to meet the Maintenance of Certification

[91] We consider a ''business day'' to include the normal work days and hours of operation during a week (Monday through Friday), excluding federal holidays and weekends.

requirement associated with enabling apps for production use discussed in more detail below.

We remind stakeholders that even in the case where an API Technology Supplier chooses not to vet app developers, the apps would *not* have carte blanche access to a health care provider's data. To the contrary, such apps will still be registered and thus be identifiable and able to have their access deactivated by an API Technology Supplier or health care provider (API Data Provider) if they behave in anomalous or malicious ways (*e.g.,* denial of service attack). And a patient seeking access to their data using the app will need to authenticate themselves (using previously issued credentials by a health care provider or trusted source) and authorize: (1) The app to connect to the FHIR server; and (2) specify the scope of the data the app may access.

As a separate matter, we also recognize that in order to assure health care providers that the apps they use within their health IT will operate appropriately, will fully integrate into workflow, and will not degrade overall system performance, that API Technology Suppliers may establish additional mechanisms to vet app developers. Such mechanisms could fit into the ''value-added services'' permitted fee and result in the app being acknowledged or listed by the health IT developer in some special manner (*e.g.,* in an ''app store,'' ''verified app'' list). While our proposals do not specify any explicit limits to the nature and governance of these approaches, we wish to caution health IT developers that even though such processes have a reasoned basis in providing an added layer of trust above and beyond the basic production-readiness of an app, they can equally be used as a means to prevent, limit, and otherwise frustrate innovation, competition, and access to the market. Such an outcome would be inconsistent with the Cures Act, could directly violate the specific Condition of Certification associated with fees permitted for value-added services, and could constitute information blocking.

iv. Permitted Fees Conditions

General Proposals Involving Fees

As part of this API Condition of Certification, we propose to adopt specific conditions that would set boundaries for the fees API Technology Suppliers would be permitted to charge and to whom those permitted fees could be charged. As a reminder, these proposals would only apply to a health IT developer's business practices associated with its ''API technology'' (*i.e.,* the capabilities certified to § 170.315(g)(7) through (11)). We seek comment on all of the following proposals.

In § 170.404(a)(3)(i)(A), we propose to establish a general prohibition on API Technology Suppliers imposing fees associated with API technology. This general prohibition is meant to ensure that API Technology Suppliers do not engage in pricing practices that create barriers to entry and competition for apps and API-based services that health care providers seek to use. These outcomes would be inconsistent with the goal of enabling API-based access, exchange, and use of EHI by patients and other stakeholders without special effort.

In establishing this general prohibition, we have been mindful of the need for API Technology Suppliers to recover their costs and to earn a reasonable return on their investments in providing API technology that has been certified under the Program. Accordingly, we have identified categories of ''permitted fees'' that API Technology Suppliers would be permitted to charge and still be compliant with the Condition of Certification and Program requirements, and discuss these proposals below. We emphasize, however, and propose in detail below, that API Technology Suppliers would not be permitted in any way whatsoever to impose fees on any person in connection with an API Technology Supplier's work to support the use of API technology to facilitate a patient's ability to access, exchange, or use their EHI.

We note that other than for fees charged for ''value-added services'' (proposed in § 170.404(a)(3)(iv)), the fees permitted under this Condition of Certification must arise between an API Technology Supplier and an API Data Provider. Any fee that arises in connection with an API User's use of API technology would need to exist solely between the API Data Provider and the API User. This policy reinforces the autonomy that we believe API Data Providers should have to establish relationships with API Users. However, as discussed in detail below, API Technology Suppliers would be permitted to charge API Data Providers based on the usage activities of API Users.

We also seek to clarify that while the proposed permitted fees set the boundaries for the fees API Technology Suppliers would be permitted to charge and to whom those permitted fees could be charged, they do not prohibit who may pay the API Technology Supplier's permitted fee. In other words, these conditions limit the party from which an API Technology Supplier may require payment, but they do not speak to who may pay the fee. For example, if through some type of relationship/agreement an API User or other party offered to pay the fee an API Data Provider owed to an API Technology Supplier, that practice would be allowed and unaffected under these conditions. This is an acceptable practice because the fee is first arrived at between the API Technology Supplier and API Data Provider, and then API Technology Supplier receives payment from another party via the API Data Provider or directly on behalf of the API Data Provider. As a general matter, we note that stakeholders should be mindful of other federal and state laws and regulations that could prohibit or limit certain types of relationships involving remuneration.

We note that the proposed ''permitted fees conditions'' align with the requirements of the information blocking exceptions proposed in 45 CFR 171.204 and 171.206. Any fee that would not be covered by those exceptions, and that would, therefore, be suspect under the information blocking provision, would equally not be permitted by this API Condition of Certification. We strongly encourage readers to review our proposals associated with those exceptions, which are contained in sections VIII.D.4 and VIII.D.6 of this preamble, respectively.

Permitted Fees—General Conditions

We propose in § 170.404(a)(3)(i)(B) general conditions that an API Technology Supplier's fee must satisfy in order for such fee to be expressly permitted and thus not contravene the proposed Condition of Certification. First, we propose in § 170.404(a)(3)(i)(B)*(1)* that in order to be a permitted fee, a fee imposed by an API Technology Supplier must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. This would require an API Technology Supplier to apply fee criteria that, among other things, would lead an API Technology Supplier to come to the same conclusion with respect to the permitted fee's amount each time it interacted with a class of persons or responded to a request. Accordingly, the fee could not be based on the API Technology Supplier's subjective judgment or discretion.

Moreover, in order to be permitted, the fee must not be based in any part on whether the API User is a competitor or potential competitor, or on whether the API Data Provider or API User will be using the data accessed via the API technology in a way that facilitates competition with the API Technology Supplier. This condition is intended to ensure that any fee charged by an API Technology Supplier does not have the purpose or effect of excluding or creating impediments for competitors, business rivals, or other persons engaged in developing or enabling the use of API technology. We believe these fee limitations are necessary in light of the potential for API Technology Suppliers to use their control over API technology to engage in discriminatory practices that create barriers to API technology. These principles are consistent with the approach described in section VIII of this preamble (''information blocking'').

Second, we propose in § 170.404(a)(3)(i)(B)*(2)* that in order to be a permitted fee, a fee imposed by an API Technology Supplier must be reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting the API technology to, or at the request of, the API Data Provider to whom the fee is charged. For example, the API Technology Supplier would not be permitted to charge a fee when the underlying costs relevant to the supply or service have already been accounted for or recovered through other fees (regardless of whether such fees were charged to the API Data Provider or to other persons). Moreover, an API Technology Supplier that conditioned access to its API technology on revenue-sharing or the entry into a royalty agreement would be at significant risk of imposing a fee that bore no plausible relation to the costs incurred by the API Technology Supplier to develop the API technology or support its use by API Users.

Third, we propose in § 170.404(a)(3)(i)(B)*(3)* to require that in order to be a permitted fee, the costs of supplying, and if applicable, supporting the API technology upon which the fee is based must be reasonably allocated among all customers to whom the API technology is supplied or for whom it is supported. A reasonable allocation of costs would require that the API Technology Supplier allocate its costs in accordance with criteria that are reasonable and between only those API Data Providers that either cause the costs to be incurred or benefit from the associated supply or support of the API technology. If an API Technology Supplier developed API technology that could be supplied to multiple customers with minimal tailoring, the core costs of developing its API technology should be allocated among those customers when recovered as a fee. The API Technology Supplier would not be permitted to recover the total of its core costs from each customer. Similarly, when an API Technology Supplier uses shared facilities and resources to support the usage of API technology, it would need to ensure that those shared costs were reasonably allocated between all of the customers that benefited from them. However, whenever an API Technology Supplier is required to provide services and incur costs that are unique to a particular customer, it would not need to distribute those costs among other customers that had deployed its API technology.

Last, we propose in § 170.404(a)(3)(i)(B)*(4)* to require that in order to be a permitted fee, the API Technology Supplier must ensure that fees are not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier. The use of such criteria would be suspect because it suggests the fee the API Technology Supplier is charging is not based on its reasonable costs to provide the API technology or services and may have the purpose or effect of excluding or creating impediments for competitors, business rivals, or other persons engaged in developing or enabling the use of API technologies and services.

We request comments on these general conditions for permitted fees and whether commenters believe we have created effective guardrails to ensure that fees do not prevent EHI from being accessed, exchanged, and used through the use of APIs without special effort.

Specific Proposed Permitted Fees

As noted above, we propose that API Technology Suppliers would be prohibited from charging fees associated with API technology unless such fees are expressly permitted. Additionally, as a reminder, the scope of ''API technology'' subject to these proposals would only include certified health IT that fulfill the API-focused certification criteria adopted or proposed for adoption at 45 CFR 170.315(g)(7) through (g)(11). Thus, all other API functionality provided by a health IT developer with its product(s) that have no link to these certified capabilities would not be subject to this Condition of Certification.

The following proposals outline the specific circumstances in which an API Technology Supplier would be permitted to charge fees associated with API technology certified under the Program. A fee that satisfies one of the permitted fees in §§ 170.404(a)(3)(ii)–(iv) must also satisfy each of the general conditions in § 170.404(a)(3)(i) in order to be permitted and for its recovery compliant with this Condition of Certification.

Permitted Fee for Developing, Deploying, and Upgrading API Technology

In § 170.404(a)(3)(ii), we propose to permit an API Technology Supplier to charge API Data Providers reasonable fees for developing, deploying, and upgrading API technology. Fees for ''developing'' API technology comprise the API Technology Supplier's costs of designing, developing, and testing API technology to specifications that fulfill the requirements of the API-focused certification criteria adopted or proposed for adoption at 45 CFR 170.315(g)(7) through (g)(11). Fees for developing API technology must not include the API Technology Supplier's costs of updating the non-API related capabilities of the API Technology Supplier's existing health IT, including its databases, as part of its development of the API technology. These costs would be connected to past business decisions made by the API Technology Supplier and typically arise due to health IT being designed or implemented in nonstandard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI. The recovery of the costs associated with updating an API Technology Supplier's health IT generally would be inconsistent with the Cures Act requirement that API technology be deployed ''without special effort.''

The API Technology Supplier's fees for ''deploying'' API technology comprise the API Technology Supplier's costs of operationalizing API technology in a production environment. Such fees include, but are not limited to, standing up hosting infrastructure, software installation and configuration, and the creation and maintenance of API Data Provider administrative functions. An API Technology Supplier's fees for ''deploying'' API technology does not include the costs associated with managing the traffic of API calls that access the API technology, which an API Technology Supplier can only recover under the permitted fee for usage support costs under § 170.404(a)(3)(iii). For clarity, we reiterate that for the purpose of this Condition of Certification, we consider that API technology is ‘‘deployed’’ by the customer—the API Data Provider—that purchased or licensed it.

The API Technology Supplier's fees for ‘‘upgrading’’ API technology comprise the API Technology Supplier's costs of supplying an API Data Provider with an updated version of API technology. Such costs would include the costs required to bring API technology into conformity with new requirements of the Program, upgrades to implement general software updates (not otherwise covered by development fees or under warranty), or developing and releasing newer versions of the API technology at the request of an API Data Provider.

The nature of the costs that can be charged under this category of permitted fees will depend on the scope of the work to be undertaken by an API Technology Supplier (*i.e.,* how much or how little labor an API Data Provider requires of the API Technology Supplier to deploy and upgrade the API technology being supplied). For example, where an API Data Provider decides to fully outsource the deployment of its API technology to its API Technology Supplier, the API Technology Supplier's costs will include the work associated with the development of the API technology, the work deploying the API technology, and any work upgrading the API technology.

We propose that any fees that an API Technology Supplier charges for developing, deploying, or upgrading API technology must be charged solely to the API Data Provider(s) for whom the capabilities are deployed. We propose this limitation because we believe that these costs should be negotiated between the API Technology Supplier that supplies the capabilities and the API Data Provider (*i.e.,* health care provider) that implements them in its production environment. In our view, it is inappropriate to pass these costs on to API Users as doing so would impose considerable costs on the API Data Provider's current or potential partners, such as those offering third-party applications and services, as well as the end-users of API technology and would amount to the kind of ‘‘special effort’’ that the Cures Act's API Condition of Certification seeks to prevent.

Subject to the general conditions proposed in § 170.404(a)(3)(i) and discussed above, API Technology Suppliers can recover the full range of reasonable costs associated with developing, deploying, and upgrading API technology over time. We believe it is important that API Technology Suppliers be able to recover these costs and earn a reasonable return on their investments so that they have adequate incentives to make continued investments in these technologies. In particular, we anticipate that API Technology Suppliers will need to continually expand the data elements and upgrade the capabilities associated with Certified APIs as the FHIR standard and its implementation specifications mature, and the National Coordinator expands the USCDI and ARCH.

Permitted Fee To Recover Costs of Supporting API Usage for Purposes Other Than Patient Access, Exchange, and Use

In § 170.404(a)(3)(iii) we propose to permit an API Technology Supplier to charge usage-based fees to API Data Providers to the extent that the API technology is used for purposes other than facilitating access, exchange, or use of EHI by patients or their applications, technologies, or services.

We consider ‘‘usage-based’’ fees to be the fees imposed by an API Technology Supplier to recover the costs that would typically be incurred supporting API interactions at increasing volumes and scale within established service levels. That is, ‘‘usage-based’’ fees recover costs incurred by an API Technology Supplier due to the actual use of the API technology once it has been deployed (*e.g.,* costs to support a higher volume of traffic, data, or number of apps via the API technology). We acknowledge that API Technology Suppliers could adopt a range of pricing methodologies when charging for the support of API usage. We expect that API usage support fees would only come into play when the API Technology Supplier acts on behalf of the API Data Provider to deploy its API technology. Thus, the costs recovered under ‘‘usage-based’’ fees would only be able to reflect ‘‘post-deployment’’ costs. As such, ‘‘usage-based’’ fees would not be allowed to include any costs necessary to prepare and ‘‘get the API technology up, running, and ready for use,’’ which are costs that we propose should be recovered as part of the deployment services delivered by the API Technology Supplier if permitted under § 170.404(a)(3)(ii). We believe this Condition of Certification offers the flexibility necessary to accommodate reasonable pricing methodologies and will allow API Technology Suppliers to explore innovative approaches to recovering the costs associated with supporting API use as a permitted fee.

As discussed above, we expect that API usage support fees would only come into play when the API Technology Supplier acts on behalf of the API Data Provider to deploy its API technology. Conversely, in scenarios where the API Data Provider, such as a large hospital system, assumes full responsibility for the technical infrastructure necessary to deploy and host the API technology it has acquired, the volume and scale of its usage would be the API Data Provider's sole responsibility. As a result, in this scenario and under our proposal's structure, an API Technology Supplier would not be permitted to charge usage-based fees. Instead, the API Technology Supplier would be limited to the fees it would be permitted to recover through the ‘‘development, deployment, upgrade’’ permitted fee discussed above.

We reiterate, that ‘‘usage-based’’ fees would need to be settled between an API Technology Supplier and API Data Provider. The API Technology Supplier would have no standing to go around or through the API Data Provider to issue fees to, for example, a population health analytics company engaged by an API Data Provider who accesses the API Data Provider's data via the API technology.

We propose that any usage-based fees associated with API technology be limited to the recovery of the API Technology Supplier's ‘‘incremental costs.’’ An API Technology Supplier's ‘‘incremental costs’’ comprise the API Technology Supplier's costs that are directly attributable to supporting API interactions at increasing volumes and scale within established service levels. We propose than an API Technology Supplier should ‘‘price’’ its costs of supporting access to the API technology by reference to the additional costs that the API Technology Supplier would incur in supporting certain volumes of API use. In practice, we expect that this means that API Technology Suppliers will offer a certain number of ‘‘free’’ API calls based on the fact that, up to a certain threshold, the API Technology Supplier will not incur any material costs in supporting API technology in addition to the costs recovered for deployment services. However, after this threshold is exceeded, we expect that the API Technology Supplier will impose usage-based costs commensurate to the additional costs that the API Technology Supplier must incur to support API technology use at increasing volumes and scale.

We expect that API Technology Suppliers would charge fees that are correlated to the incremental ratchetting up of the cost required to meet increased demand. For example, if, at a certain volume of API calls, the API Technology Supplier needed to deploy additional server capacity, the associated incremental cost of bringing an additional server online could be passed on to the API Data Provider because the API technology deployed on behalf of the API Data Provider was the subject of the higher usage. Up until the point that the threshold is reached, the additional server capacity was not required and so the API Technology Supplier would not be permitted to recover the cost associated with it. Moreover, the additional server capacity would support ongoing demand up to a certain additional volume, and so the API Technology Supplier would not be permitted to recover the costs of further additional server capacity until the then current capacity was exhausted.

Notwithstanding the above, we note that API Technology Suppliers may choose to charge for their API usage support services on a ''pay as you go'' basis, such as a fee-per-call pricing structure. This approach could be consistent with the requirement that the API Technology Supplier only impose its incremental costs, and the requirements of this Condition of Certification more generally. However, depending on the amount being charged, this pricing model is open to abuse, with API Data Providers at risk of paying unreasonably high fees if the volume of API use is high and when the API Data Provider does not share in the benefits enjoyed by the API Technology Supplier when delivering a service at scale. As such, the API Technology Supplier would need to be careful to ensure that the total fees paid by an API Data Provider were reasonably related to the API Technology Supplier's costs of supporting the API technology. Where the fees paid over a reasonable measuring period were not reasonably related to the API Technology Supplier's costs, they would not be permitted.

We are also aware that API Technology Suppliers may offer a pricing structure for API usage support based on unlimited API calls. That is, the API Technology Supplier may charge a flat-fee irrespective of the volume of traffic accessing the API technology. Such a pricing model would be allowed under the proposed condition provided that the API Technology Supplier's fee for API usage support was reasonably related to the cost of the services that it had agreed to provide. This would mean that the API Technology Supplier would need to make a realistic estimate of the volume of API calls that it would need to support to fulfill any service level promised, and calculate its fee based on the costs of supporting that call volume. So long as the API Technology Supplier made a realistic estimate of the anticipated volume and support level, the legitimacy of the API Technology Supplier's fees, and its ability to recover them as permitted fees, would be unaffected by API Users making lower than expected use of API technology.

In the context of this proposed permitted fee's scope and the proposed general prohibition on fees, we seek to make clear that API Technology Suppliers would be prohibited from charging (or including in their contracts and agreements with API Data Providers) any usage-based fees for API uses that are associated with the access, exchange, and use of EHI by patients or their applications, technologies, or services. This would include, among other things, API calls or other transactions initiated by or on behalf of a patient, including third parties (*e.g.,* an application or any other technology or service) authorized by the patient or their representative to request data on their behalf.

Usage fees associated with the access, exchange, and use of EHI by patients is a specific example of a prohibited fee that would fit under the general prohibition of a ''fee not otherwise permitted'' and is based on several considerations. First, such fees between an API Technology Supplier and API Data Provider would likely be passed on directly to patients, creating a significant impediment to their ability to access, exchange, and use their EHI, without special effort, through applications and technologies of their choice. More fundamentally, most of the information contained in a patient's electronic record has been documented during the practice of medicine or has otherwise been captured in the course of providing health care services to patients. In our view, patients have effectively paid for this information, either directly or through their employers, health plans, and other entities that negotiate and purchase health care items and services on their behalf. Thus, our proposal reflects our belief that it is inappropriate to charge patients additional costs to access this information, whether those costs are charged directly to patients or passed on as a result of fees charged to persons that provide apps, technologies, and services on a patient's behalf.

To be clear, if an API Data Provider sought to employ API technology for the limited purpose of making EHI available to patients and their apps, the API Data Provider's API Technology Supplier would have no legitimate basis to charge the API Data Provider, or any other person, for the ''patient access'' usage-based costs associated with the API technology.

Any unreasonable fees associated with a patient's access to their EHI may be suspect under the information blocking provision. Such fees may also be inconsistent with an individual's right of access to their PHI under the HIPAA Privacy Rule (45 CFR 164.524).)

In addition to our proposal in § 170.404(a)(3)(iii)(A) and detailed above that this permitted fee would not include any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information, we also propose to explicitly exclude two additional costs from this permitted fee. In § 170.404(a)(3)(iii)(B), we propose that this permitted fee would not include costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets. For instance, an API Technology Supplier could not charge an API Data Provider a fee based on the purported ''cost'' of allowing the API Data Provider to use the API Technology Supplier's patented API technology. As discussed in more detail in section VIII.D.4 (Information Blocking), we believe it would be inappropriate to permit an actor to charge a fee based on these considerations, which are inherently subjective and could invite the kinds of rent-seeking and opportunistic pricing practices that create barriers to access, use, and exchange of EHI and impede interoperability.

In § 170.404(a)(3)(iii)(C), we propose that this permitted fee would not include opportunity costs, except for the reasonable forward-looking cost of capital. These speculative costs could include revenues that an API Technology Supplier could have earned had it not provided the API technology. We clarify that the exclusion of opportunity costs would not preclude an API Technology Supplier from recovering its reasonable forward-looking cost of capital. We believe these costs are relatively concrete and that permitting their recovery will protect incentives for API Technology Suppliers to invest in developing and providing interoperability elements (as described in section VIII.D.4).

Permitted Fee for Value-Added Services

In § 170.404(a)(3)(iv) we propose to permit an API Technology Supplier to charge fees to API Users[92] for value-

[92] In this context a health care provider, which could otherwise be an ''API Data Provider'' in one context, may equally be an API User in a different

added services supplied in connection with software that can interact with the API technology. These ‘‘value-added services’’ would need to be provided in connection with and supplemental to the development, testing, and deployment of software applications that interact with API technology. Critically, fees would not be permitted if they interfere with an API User's ability to efficiently and effectively develop and deploy production-ready software. This means that in order to be permitted, an API User could not be required to incur the fee in order to develop and deploy a production-ready software application that interacts with the API technology acquired by the API Data Provider. Rather, a fee will only be permitted if it relates to a service that a software developer can elect to purchase, but is not required to purchase in order to develop and deploy production-ready apps.

We believe it appropriate to permit this type of fee because API Technology Suppliers may offer a wide-range of market differentiating services to make it attractive for API Users to develop software applications that can interact with the API technology supplied by an API Technology Supplier. Such services could include advanced training, premium development tools and distribution channels, and enhanced compatibility/integration testing assessments. For example, an API Technology Supplier would be permitted to charge fees for value-added services that would be associated with but go beyond the scope set by the (g)(10)–certified API, such as write access, co-branded integration into the API Technology Supplier's product(s) workflow, co-marketing arrangements, and promoted placement in an API Technology Supplier's app store. That said, we caution API Technology Suppliers that value-added services would have to be made available in a manner that complies with other requirements of this Condition of Certification and with the information blocking provision.

To illustrate the scope of the fees permitted under this proposal, we clarify that the permitted value-added services fee would enable an API Technology Supplier to recover certain costs associated with operating an ‘‘app store.’’ However, those fees cannot interfere with an API User's ability to efficiently and effectively develop and deploy production-ready apps without special effort. We are aware that API Technology Suppliers offer services associated with the listing and promotion of apps beyond basic app placement. Such fees would be permitted, so long as the API Technology Supplier ensured that basic access and listing in the app store was provided free of charge if an app developer depended on such listing to efficiently and effectively develop and deploy production-ready apps without special effort. Fees charged for additional/specialized technical support or promotion of the API User's app beyond these basic access and listing services would also be permitted. In contrast, if an API Technology Supplier required, for example, a software developer's app to go through a paid listing process as a dependency/precondition to be able to be deployed (and generally accessible) to the API Technology Supplier's health care provider customers to use, this would not be a permitted fee under this Condition of Certification, would constitute special effort, and could raise information blocking concerns.

Prohibited Fees

As discussed above, we proposed that any API-related fee imposed by an API Technology Supplier that is not expressly permitted is prohibited. This approach is necessary because, as discussed in section VIII.C.5.c of this proposed rule, we continue to receive evidence that some health IT developers are engaging in practices that create special effort when it comes to API technology. These practices include fees that create barriers to entry or competition as well as rent-seeking and other opportunistic behaviors. For example, some health IT developers are conditioning access to technical interoperability documentation on revenue-sharing or royalty agreements that bear no plausible relation to the costs incurred by the health IT developer to provide or enable its use. We are also aware of discriminatory pricing policies that have the purpose or effect of excluding competitors from the use of APIs and other interoperability elements. These practices close off the market to innovative applications and services that could empower patients and enable providers to deliver greater value and choice to health care consumers and additional service providers.

To address these concerns we provide the following non-exhaustive examples of fees for services that API Technology Suppliers would be prohibited from charging:

- Any fee for access to the documentation that an API Technology Supplier is required to publish or make available under this Condition of Certification.
- Any fee for access to other types of documentation or information that a software developer may reasonably require to make effective use of API technology for any legally permissible purpose.
- Any fee in connection with any services that would be essential to a developer or other person's ability to develop and commercially distribute production-ready applications that use API technology. These services could include, for example, access to ‘‘test environments’’ and other resources that an app developer would need to efficiently design and develop apps. The services could also include access to distribution channels if they are necessary to deploy production-ready software and to production resources, such as the information needed to connect to FHIR servers (endpoints) or the ability to dynamically register with an authorization server.

Permitted Fees Request for Comment

We request comment on any additional specific ‘‘permitted fees’’ not addressed above that API Technology Suppliers should be able to recover in order to assure a reasonable return on investment. Furthermore, we request comment on whether it would be prudent to adopt specific, or more granular, cost methodologies for the calculation of the permitted fees. Commenters are encouraged to consider, in particular, whether the approach we have described will be administrable and appropriately balance the need to ensure that patients, providers, app developers, and other stakeholders do not encounter unnecessary costs and other special effort with the need to provide adequate assurance to API Technology Suppliers, investors, and innovators that they will be able to earn a reasonable return on their investments in API technology. We welcome comments on whether the approach adequately balances these concerns or would achieve our stated policy goals, and we welcome comments on potential revisions or alternative approaches. We encourage detailed comments that include, where possible, economic justifications for suggested revisions or alternative approaches.

Record-Keeping Requirements

To provide appropriate accountability, we propose in § 170.404(a)(3)(v) that API Technology Suppliers must keep for inspection

context. Given this potential dual role for health care providers, we have focused on API Users as the party to whom a fee may be charged for the purposes of this permitted fee.

detailed records of all fees charged with respect to API technology and all costs that it claims to have incurred to provide API technology to API Data Providers. To provide assurance that the API Technology Supplier's fees are reasonably related to the API Technology Supplier's costs, the API Technology Supplier would need to document, with the same level of detail, any fees charged and associated costs incurred to provide other services to which any portion of the costs could reasonably be attributed. For example, if the API Technology Supplier charges a fee that reflects its costs for internet servers used to provide the API technology, the API Technology Supplier would need to document the costs of any other internet-based services it provides, as well as any other purposes for which the internet servers are used.

Separately, an API Technology Supplier would need to document the criteria it used to allocate any costs across relevant customers, requestors, or other persons. The criteria must be documented in a level of detail that would enable determination as to whether the API Technology Supplier's cost allocations are objectively reasonable and comply with the cost accountability requirements, including whether fees reflect the API Technology Supplier's actual costs reasonably incurred, were allocated reasonably and between only those API Data Providers that either cause the costs to be incurred or benefit from the associated supply or support of the API technology, and were distributed across customers and other relevant persons in a permissible manner, as described above.

We note that an API Technology Supplier must retain its accounting records consistent with the retention requirement proposed for adoption as part of the Assurances Condition of Certification (proposed for adoption in § 170.402). In the event that a potential violation of this Condition and Maintenance of Certification creates a conformance fact-finding scenario by ONC or information blocking is investigated, we believe that this period of time would provide ONC with appropriate visibility into the API Technology Supplier's business practices.

We request comment on whether these requirements provide adequate traceability and accountability for costs permitted under this API Condition of Certification. We also seek comment on whether to require more detailed accounting records or to prescribe specific accounting standards.

iv. Openness and Pro-Competitive Conditions

We propose that API Technology Suppliers would have to comply with certain requirements to promote an open and competitive marketplace. As a general condition, we propose in § 170.404(a)(4) that API Technology Suppliers must grant API Data Providers (*i.e.,* health care providers who purchase or license API technology) the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider. We reinforce this general condition through more specific proposed conditions proposals discussed below that would require API Technology Suppliers to provide equitable access to API technology, which would include granting the rights and providing the cooperation necessary to enable apps to be deployed that use the API technology to access, exchange, and use EHI in production environments.

As important context for these proposals, we note that the API technology required by this Condition of Certification falls squarely within the concept of ''essential interoperability elements'' described in section VIII.C.4.b of this preamble and, as such, are subject to strict protections under the information blocking provision. As a corollary, to the extent that API Technology Suppliers claim an intellectual property right or other proprietary interest in the API technology, they must take care not to impose any fees, require any license terms, or engage in any other practices that could add unnecessary cost, difficulty, or other burden that could impede the effective use of the API technology for the purpose of enabling or facilitating access, exchange, or use of EHI. Moreover, even apart from these information blocking considerations, we believe that, as developers of technology certified under the Program, API Technology Suppliers owe a special responsibility to patients, providers, and other stakeholders to make API technology available in a manner that is truly ''open'' and minimizes any costs or other burdens that could result in special effort. The proposed conditions set forth below are intended to provide clear rules and expectations for API Technology Suppliers so that they can meet these obligations.

Non-Discrimination

We propose in § 170.404(a)(4)(i) that an API Technology Supplier must adhere to a strictly non-discriminatory policy regarding the provision of API technology. As a starting point, we propose to require in § 170.404(a)(4)(i)(A) that API Technology Suppliers comply with all of the requirements discussed in section VIII.C.4.b of this proposed rule regarding the non-discriminatory provision of interoperability elements. Accordingly, and consistent with developers' obligations under the Program and our expectation that API technology be truly ''open,'' we propose to require that API Technology Suppliers must provide API technology to API Data Providers on terms that are no less favorable than they would provide to themselves and their customers, suppliers, partners, and other persons with whom they have a business relationship. This requirement would apply to both price and non-price terms and thus would apply to any fees that the API Technology Supplier is permitted to charge under the ''permitted charges conditions'' of this Condition of Certification. We believe this requirement would ensure that API Data Providers (*i.e.,* health care providers) who purchase or license API technology have sole authority and autonomy to permit third-party software developers to connect to and use the API technology they have acquired.

Next, we propose in § 170.404(a)(4)(i)(B) that any terms and conditions associated with API technology would have to be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. For example, if the API Technology Supplier applied an ''app store'' entry/listing process unequally and added arbitrary criteria based on the use case(s) an app was focused on, such business practices would not comply with this specific condition and could also be in violation of the information blocking provision.

Moreover, we propose in § 170.404(a)(4)(i)(C) that an API Technology Supplier would be prohibited from offering or varying such terms or conditions on the basis of impermissible criteria, such as whether the API User with whom the API Data Provider has a relationship is a competitor, potential competitor, or will be using EHI obtained via the API technology in a way that facilitates competition with the API Technology Supplier. The API Technology Supplier would also be prohibited from taking into consideration the revenue or other value the API User with whom the API Data Provider has a relationship may derive from access, exchange, or use of EHI obtained by means of the API technology. We believe these proposals will help promote greater equity and competition in market as well as prevent discriminatory business practices by API Technology Suppliers.

Rights To Access and Use API Technology

We propose in § 170.404(a)(4)(ii)(A) that an API Technology Supplier would have to make API technology available in a manner that enables API Data Providers and API Users to develop and deploy apps to access, exchange, and use EHI in production environments. To this end, we propose that an API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment. In other words, this proposal is focused on the provision of rights reasonably necessary to access and use API technology and does not extend to other intellectual property maintained by the API Technology Supplier, especially intellectual property that has no nexus with the access and use of API technology. In situations where such a nexus exists, even partially, the API Technology Supplier would have the duty to determine a method to grant the applicable rights reasonably necessary to access and use the API technology. And if practicable, under these partial cases, we note that it would be possible for the API Technology Supplier to exclude the intellectual property that would have no impact on the access and use of the API technology.

Accordingly, following our proposal, API Technology Suppliers would need to grant API Data Providers and their API Users with rights that could include but not be limited to the following in order to sufficiently support the use of the API technology:

- For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier's health IT or with health IT under the API Technology Supplier's control.
- Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment. Note, API Technology Suppliers, pursuant to the ''value-added services'' permitted fee, would be able to offer and charge for services such as preferential marketing agreements, co-marketing agreements, and other business arrangements so long as such services are beyond what is necessary for the API technology to be put into use in a production environment.
- Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

Relatedly, in § 170.404(a)(4)(ii)(B) we propose to prohibit an API Technology Supplier from imposing any collateral terms or agreements that could interfere with or lead to special effort in the use of API technology for any of the above purposes. We note that these collateral terms or agreements may also implicate the information blocking provision for the reasons described in section VIII.D.3.c of this preamble. These specific proposed conditions would expressly prohibit an API Technology Supplier from conditioning any of the rights described above on the requirement that the recipient of the rights do, or agree to do, any of the following:

- Pay a fee to license the rights described above, including but not limited to a license fee, royalty, or revenue-sharing arrangement.
- Not compete with the API Technology Supplier in any product, service, or market.
- Deal exclusively with the API Technology Supplier in any product, service, or market.
- Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.
- License, grant, assign, or transfer any intellectual property to the API Technology Supplier.
- Meet additional developer or product certification requirements.
- Provide the API Technology Supplier or its technology with reciprocal access to application data.

These prohibitions largely mirror those proposed under the exception to the information blocking definition in § 171.206 and reflect the same concerns expressed in that context in section VIII.D.3.c of this preamble. However, we note the following important distinction: Whereas proposed § 171.206 would permit a developer to charge a reasonable royalty to license interoperability elements, this API Condition of Certification would not permit any such royalty, license fee, or other type of fee of any kind whatsoever pursuant to the general fee prohibition proposed in the ''permitted charges condition.'' This additional limitation reflects the more exacting standards that apply to API Technology Suppliers with respect to the provision of API technology under this Condition of Certification. While we believe that, for the reasons described in section VIII.D.3.c of this preamble, health IT developers should generally be permitted to charge reasonable royalties for the use of their intellectual property, we consider API technology to be a special case. Certified health IT developers (*i.e.,* API Technology Suppliers) are required to provide these capabilities as part of their statutory duty to facilitate the access, exchange, and use of patient health information from EHRs ''without special effort.'' We believe the language requiring that these capabilities be ''open'' precludes an API Technology Supplier from conditioning access to API technology on the payment of a royalty or other fee, however ''reasonable'' the fee might otherwise be.

We clarify that the prohibitions explained above against additional developer or Health IT Module certification requirements and, separately, against requirements for reciprocal access to application data, are within the scope of the collateral terms prohibited by proposed § 171.206 even though these additional API Technology Supplier requirements are not explicitly referenced by that exception because they are not generally applicable to all types of interoperability elements. Nevertheless, permitting an API Technology Supplier to impose these kinds of additional requirements would be inconsistent with the Cures Act's expectation that API technology be made available openly and in a manner that promotes competition. For the same reason such practices may raise information blocking concerns.

API Technology Suppliers—Additional Obligations

To support the use of API technology in production environments, we propose in § 170.404(a)(4)(iii) that an API Technology Supplier must provide all support and other services that are reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and its API Users in production environments. In general, the precise nature of these obligations will depend on the specifics of the API Technology Supplier's technology and the manner in which it is implemented and made available for specific customers. Therefore, with the following exceptions, we do not delineate the API Technology Supplier's specific support obligations and instead propose a general requirement to this effect in § 170.404(a)(4)(iii).

Changes and Updates to API Technology and Terms and Conditions

We propose to require in § 170.404(a)(4)(iii)(A) that API Technology Suppliers must make reasonable efforts to maintain the compatibility of the API technology they develop and assist API Data Providers to deploy in order to avoid disrupting the use of API technology. Similarly, we propose in § 170.404(a)(4)(iii)(B) that prior to making changes or updates to its API technology or to the terms or conditions thereof, an API Technology Supplier would need to provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with its API technology or to comply with any revised terms or conditions. Without this opportunity, clinical and patient applications could be rendered inoperable or operate in unexpected ways unbeknownst to the users or software developers.

Further, we note that this proposal aligns with the exception to the information blocking definition proposed in § 171.206. As explained in section VIII.D.3.c of this preamble, the information blocking definition would be implicated were an API Technology Supplier to make changes to its API technology that ''break'' compatibility or otherwise degrade the performance or interoperability of the licensee's products or services that incorporate the licensed API technology. We propose these additional safeguards are important in light of the ease with which an API Technology Supplier could make subtle ''tweaks'' to its technology or related services, which could disrupt the use of the licensee's compatible technologies or services and result in substantial competitive and consumer injury.

We clarify that this requirement would in no way prevent an API Technology Supplier from making improvements to its technology or responding to the needs of its own customers or users. However, the API Technology Supplier would need to demonstrate that whatever actions it took were necessary to accomplish these purposes and that it afforded the licensee a reasonable opportunity under the circumstances to update its technology to maintain interoperability. Relatedly, we recognize that an API Technology Supplier may have to suspend access or make other changes immediately and without prior notice in response to legitimate privacy, security, or patient safety-related exigencies. Such practices would be permitted by this Condition of Certification provided they are tailored and do not unnecessarily interfere with the use of API technology. From an information blocking standpoint, if such practices interfered with access, exchange, or use of EHI, the API Technology Supplier could seek coverage under the exceptions to the information blocking provision described in section VIII.D of this preamble. For instance, if the suspended access was in response to a privacy exigency, the API Technology Supplier may be able to seek coverage under the exception for promoting the privacy of EHI at proposed § 171.202.

e. Maintenance of Certification Requirements

We propose to adopt Maintenance requirements for this Condition of Certification. These maintenance requirements would be duties that we believe the Cures Act expected API Technology Suppliers (*i.e.,* health IT developers) would need to comply with in the course of maintaining their Health IT Module(s)' certification.

i. App Registration Timeliness

In the specific context of application registration, we wish to underscore that to provide a frictionless experience for developers of these applications and individuals that use them, an API Technology Supplier would be required to provide all services and other support necessary to ensure that such apps can be deployed and used in production without any additional assistance or intervention by the API Technology Supplier. For this reason, we propose in § 170.404(b)(1) a specific requirement for API Technology Suppliers that they would need to ''register'' (in connection with the API technology functionality proposed in § 170.315(g)(10)(iii)) and enable all applications for production use within one business day of completing its verification of an application developer's authenticity as described in proposed § 170.404(a)(2)(ii)(C). We propose this explicit requirement is necessary in order to ensure that a patient's ability to use an app of their choice is not artificially or intentionally slowed by an API Technology Supplier, causing special effort on the part of the patient to gain access to their EHI. We also emphasize that this is specific duty for API Technology Suppliers in the course of maintaining the Health IT Module(s)' certificate to which their API technology is associated. In instances where an API Technology Supplier chooses not to perform app developer verification processes described in proposed § 170.404(a)(2)(ii)(C), it would need to solely meet this one business day requirement from the point of having received a request for registration.

ii. Publication of FHIR Endpoints

In order to interact with a FHIR RESTful API, an app needs to know the ''FHIR Service Base URL,'' which is often referred to colloquially as a ''FHIR server's endpoint.'' [93] The public availability and easy accessibility of this information is a central necessity to assuring the use of FHIR-based APIs without special effort, especially for patient access apps. Accordingly, we propose to adopt in § 170.404(b)(2) a specific requirement that an API Technology Supplier must support the publication of Service Base URLs for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed, and make such information publicly available (in a computable format) at no charge. In instances where an API Technology Supplier is contracted by an API Data Provider to manage its FHIR server, we expect that this administrative duty will be relatively easy to manage. In instances where an API Data Provider assumes full responsibility to ''locally manage'' its FHIR server, the API Technology Supplier would be required, pursuant to this proposed maintenance requirement, to obtain this information from its customers. We strongly encourage API Technology Suppliers, health care providers, HINs and patient advocacy organizations to coalesce around the development of a public resource or service from which all stakeholders could benefit. We believe this would help scale and enhance the ease with which Service Base URLs could be obtained and used.

iii. Providing (g)(10)–Certified APIs to API Data Providers

We propose in § 170.404(b)(3) that an API Technology Supplier with API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Data Providers with such API technology deployed with API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of this final rule's effective date. We believe this Maintenance of Certification requirement will permit ONC to monitor and facilitate the rollout to health care providers of this important functionality. This is of particular relevance as we propose below to include this functionality in the 2015 Base EHR definition in place of the

[93] *http://hl7.org/fhir/http.html#general.*

current ''application access—data category request'' certification criterion (§ 170.315(g)(8)), which means health care providers will need this functionality to meet the Certified EHR Technology (CEHRT) for associated Centers for Medicare & Medicaid Services (CMS) programs.

f. 2015 Edition Base EHR Definition

As described in detail above, we have propose to adopt a new certification criterion in § 170.315(g)(10) that would replace the current criterion adopted in § 170.315(g)(8) and as referenced in the 2015 Edition Base EHR definition expressed in § 170.102. This change is necessary to fully implement the Cures Act and ensure that API Technology Suppliers have the requisite incentive to deploy standardized APIs that can be used ''without special effort'' and API Data Providers have added incentive to adopt such functionality. As result, we propose to create a phase-in for the proposed API certification criterion in § 170.315(g)(10) from the issuance of a subsequent final rule. This phase-in period includes separate and sequential time for API Technology Suppliers and API Data Providers.

Consistent with our proposed compliance timing for the certification criterion proposed for adoption in § 170.315(b)(10), we propose to add compliance timeline language to the 2015 Edition Base EHR definition for the transition from § 170.315(g)(8) to § 170.315(g)(10) that would reflect a total of 24 months from the final rule's effective date (which practically speaking would be 25 months because of the 30-day delayed effective date). We believe this approach is best because it identifies a single, specific date for both API Technology Suppliers and API Data Providers by which upgraded API technology needs to be deployed in production. We also believe that 24 months is sufficient for this upgrade because the scope and nature of our proposals intersect and reflect a large portion of capabilities API Technology Suppliers have already developed and deployed to meet § 170.315(g)(8). Moreover, this single date enables API Technology Suppliers (based on their client base and IT architecture) to determine the most appropriate timeline for development, testing, certification, and product release cycles in comparison to having to meet an arbitrary ''must be certified by this date'' requirement.

5. Real World Testing

The Cures Act requires, as a Condition and Maintenance of Certification under the Program, that health IT developers have successfully tested the real world use of the technology for interoperability in the type of setting in which such technology would be marketed. The Cures Act defines interoperability as ''health information technology that enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and does not constitute information blocking as also defined by the Cures Act.'' [94] We propose to codify this interoperability definition in § 170.102. We further note that we propose in section VIII of this proposed rule to codify the definition of information blocking included in the Cures Act in § 171.103.

The Program issues, and will continue to issue under our real world testing approach, certifications to health IT through a process whereby health IT is assessed against the testing requirements established by ONC. Often, this means health IT is tested by an ONC–ATL in a laboratory environment through methods that include a testing proctor's visual inspection of functions, review of developer-provided documentation of functions, and testing tools with simulation test data. An ONC–ACB evaluates the results of testing and makes a determination, based on these test results and an assessment of compliance with other Program requirements, to issue the health IT a certificate. Over the course of the Program's existence, ONC has emphasized the continued conformance of certified health IT products post-certification in real world and clinical settings. For example, ONC expanded the responsibilities of ONC–ACBs in the 2015 Edition final rule to require that they perform in-the-field surveillance. We did this to affirm the Program's long-standing expectations that certified health IT continue to operate in accordance with certification requirements when implemented in the field (80 FR 62707–62719). These efforts are also in line with the Cures Act's real world testing Condition of Certification through their focus on system interoperability and exchange of information as deployed and used in care environments—that is to say, in the ''real world.''

The objective of real world testing is to verify the extent to which certified health IT deployed in operational production settings is demonstrating continued compliance to certification criteria and functioning with the intended use cases as part of the overall maintenance of a health IT's certification. Real world testing should ensure certified health IT has the ability to share electronic health information with other systems. Real world testing should assess that the certified health IT is meeting the intended use case(s) of the certification criteria to which it is certified within the workflow, health IT architecture, and care/practice setting in which the health IT is implemented. Accordingly, we propose that successful real world testing means for the purpose of this Condition of Certification that:

- The certified health IT continues to be compliant to the certification criteria to which it is certified, including the required technical standards and vocabulary codes sets;
- The certified health IT is exchanging electronic health information in the care and practice settings for which it is intended for use; and
- Electronic health information is received by and used in the certified health IT.

We propose to limit the applicability of this Condition of Certification to health IT developers with Health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange, which are:

- The care coordination criteria in § 170.315(b);
- The clinical quality measures (CQMs) criteria in § 170.315(c)(1) through (c)(3);
- The ''view, download, and transmit to 3rd party'' criterion in § 170.315(e)(1);
- The public health criteria in § 170.315(f);
- The application programming interface criteria in § 170.315(g)(7) through (g)(11); and
- The transport methods and other protocols criteria in § 170.315(h).

The 2015 Edition certification criteria that are not included in the proposed list include many functionality-based criteria, administrative criteria, and, overall, criteria that do not focus on interoperability *and* exchange of data. In particular, we do not propose to include the 2015 Edition paragraph (a) ''clinical'' certification criteria in this list because they do not focus on interoperability and exchange of data. However, the data in the paragraph (a) criteria largely will be covered through the USCDI as a minimum data set expected for exchange; the USCDI is included in such criteria as ''transitions

[94] Defined in Section 3022 of the Cures Act.

of care'' (§ 170.315(b)(1)), ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1)), and the API criteria (*i.e.,* § 170.315(g)(9) and (10)).

We solicit comment on whether to include the ''patient health information capture'' certification criteria in § 170.315(e)(3), including the value of real world testing these functionalities compared to the benefit for interoperability and exchange. We also solicit comment on whether any other 2015 Edition certification criteria should be included or removed from the applicability list for this Condition of Certification.

To fully implement the real world testing Condition of Certification as described above, we propose Maintenance of Certification requirements that would require health IT developers to submit publicly available prospective annual real world testing plans and retrospective annual real world testing results for its certified health IT that include certification criteria focused on interoperability. As we considered the various approaches to implement this Cures Act requirement on health IT developers, we determined that health IT developers would be best positioned to construct how their certified health IT could be tested in the real world. Moreover, by requiring health IT developers to be responsible for facilitating their certified health IT testing in production settings and being held accountable to publicly publish their results, we would balance the respective burden of this statutory requirement with its intended assurances for health care providers. Additionally, ONC is not adequately resourced to centrally administer a real world testing regime among each health IT developer and its customers, nor do we have the specific relationships with health care providers that health IT developers do. Lastly, even if ONC were positioned to support and scale a real world testing regime, we would run the risk of having one-size-fits-all tools that would not necessarily get to the level of detail and granularity necessary and reflective of different health care settings and different scopes of practice that use certified health IT.

Given these considerations, we propose that a health IT developer must submit an annual real world testing plan to its ONC–ACB via a publicly accessible hyperlink no later than December 15, of each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria specified for this Condition of Certification. Prior to submission to the ONC–ACB, the plan would need to be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information. The plan would need to include all health IT certified to the 2015 Edition through August 31 of the preceding year. The plan would also need to address the health IT developer's real world testing for the upcoming calendar year and include, for each of the certification criteria in scope:

- The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability, including a mandatory focus on scenario- and use case-focused testing;
- The care and practice setting(s) that will be tested for real world interoperability, including conformance to certification criteria requirements, and an explanation for the health IT developer's choice of care setting(s) to test; [95]
- The timeline and plans for voluntary updates to standards and implementation specifications that ONC has approved (further discussed below);
- A schedule of key real world testing milestones;
- A description of the expected outcomes of real world testing;
- At least one measurement/metric associated with the real world testing; and
- A justification for the health IT developer's real world testing approach.

The intended testing methods/methodologies would need to address testing scenarios, use cases, and workflows associated with interoperability. Testing may occur in the operational setting using real patient data, in an environment that mirrors the clinical setting using synthetic or real patient data, or in the clinical setting with synthetic data intermixed. Note that when Health IT developers who are HIPAA business associates are conducting testing using ePHI, such testing must be conducted consistent with their business associate agreements and other compliance responsibilities. The health IT developer may also partner with other health IT developers to perform real world testing. We would expect developers to consider such factors as the size of the organization that production systems support, the type of organization and setting, the number of patient records and users, system components and integrations, and the volume and types of data exchange in planning for real world testing. We would also expect developers to explain how they will incorporate voluntary standards updates in their real world testing as discussed further below. While we are not proposing a minimum proportion of the customer base that must be covered in real world testing, we highly encourage developers to find ways to ensure, to the extent practical, proportionate coverage of their customer base that balances the goals of real world testing with burden to providers. Health IT developers would not be required to test the certified health IT in each and every setting in which it is intended for use as this would likely not be feasible due to the associated burden; however, developers must address their choice of care and/or practice settings to test and ONC encourages developers test in as many settings as feasible. Additionally, health IT developers would be required to provide a justification for their chosen approach. Because our approach provides great flexibility for health IT developers with respect to demonstrating compliance, we believe it is imperative that they provide a justification to explain their methodology. Through the transparent reporting of their real world testing plans, the public will have an opportunity to consider a health IT developer's chosen approach(es) and whether it is sufficiently comprehensive to provide assurance that the certified health IT has satisfactorily demonstrated its satisfaction of Program requirements including interoperability in real world settings relevant to their needs.

Health IT developers should consider existing testing tools and approaches that may be used to assess real world interoperability. For example, we encourage health IT developers to consider metrics of use and exchange from existing networks, communities, and tools including, but not limited to, Surescripts, Carequality, CommonWell Health Alliance, the C–CDA One-Click Scorecard, and DirectTrust. We do not believe that testing through the ONC-approved test procedures is sufficient to demonstrate real world use as the test procedures developed for initial laboratory testing and certification are generally setting agnostic, focused on standards conformance, and do not always test the full scope of the certification criteria's intended functionality. We also clarify that the

[95] We do not propose to specifically define or limit the care settings and leave it to the health IT developer to determine. As an example, health IT developers can consider categories, including but not limited to, those used in the EHR Incentive Programs (*https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/October2017_MedicareEHRIncentivePayments.pdf*); long-term and post-acute care; pediatrics; behavioral health; and small, rural, and underserved settings.

ONC-approved test procedures are not intended for use in in-the-field surveillance or for real world testing. Further, we do not believe connect-a-thons are a valid approach to testing real world use of health IT because they do not necessarily assess interoperability and functionality in live settings, but rather test developer/vendor connectivity in a closed test environment. Health IT developers may consider working with an ONC–ACB to have the ONC–ACB oversee the execution of the health IT developer's real world testing plans, which could include in-the-field surveillance per § 170.556, as an acceptable approach to meet the requirements of the real world testing Condition of Certification.

We propose that health IT developers with multiple certified health IT products that may include the same interoperability-focused certification criteria intended to be implemented in the same settings have the discretion to design their real world testing plans in a way that efficiently tests a combination of products. Likewise, health IT developers may find portions of their real world testing plans are transferrable to their other certified products; thus a health IT developer could choose to submit a real world testing plan that covers multiple certified products as appropriate and as long as there is traceability to the specific certified Health IT Modules. To be clear, developers of health IT products deployed through the cloud who offer their products for multiple types of settings would be required to test the same capability for those different settings. However, we solicit comment on whether we should offer an exemption for services that truly support all of a developer's customers through a single interface/engine and whether this would be sufficient to meet the intent of the real world testing Condition of Certification. Additionally, while the developers' plans must address each of the interoperability-focused certification criteria in their certified health IT, developers can and should design scenario-based test cases that incorporate multiple functionalities as appropriate for the real world workflow and setting.

We propose that a health IT developer would submit annual real world testing results to their ONC–ACBs via a publicly accessible hyperlink no later than January 31, of each calendar year for the preceding calendar year's real world testing. Real world testing results for each interoperability-focused certification criterion must address the elements required in the previous year's testing plan, describe the outcomes of real world testing with any challenges encountered, and provide at least one measurement or metric associated with the real world testing. As noted above, developers are encouraged to use metrics demonstrating real world use from existing networks and communities. We seek comment on whether ONC should require developers submit real world testing results for a minimum ''core'' set of general metrics/measurements and examples of suggested metrics/measurements. We also invite comment on the proposed annual frequency and timing of required real world testing results reporting.

We acknowledge that a subsequent final rule for this proposed rule may not provide sufficient time for health IT developers to develop and submit plans for a full year of real world testing in 2020. If such a situation comes to fruition, we expect to provide an appropriate period of time for developers to submit their plans and potentially treat 2020 as a ''pilot'' year for real world testing. We would expect that such pilot testing conform to our proposed real world testing to the extent practical and feasible (*e.g.,* same criteria but for a shorter duration and without the same consequences for non-compliance). We welcome comments on this potential approach.

We clarify, and propose, that even if a health IT developer does not have customers or has not deployed their certified Health IT Module at the time the real world testing plan is due, the health IT developer would still need to submit a plan that addresses its prospective testing for the coming year for any health IT certified prior to August 31 of the preceding calendar year. If a health IT developer does not have customers or has not deployed their certified Health IT Module when the annual real world testing results are due, we propose that the developer would need to report as such to meet the proposed Maintenance of Certification requirement. For further clarity, a developer would not need to report on any health IT certified after August 31, in the preceding year.

Standards Version Advancement Process

As new and more advanced versions[96] become available for adopted standards and implementation specifications applicable to criteria subject to the real world testing Condition and Maintenance of Certification Requirements, we believe that a health IT developer's ability to conduct ongoing maintenance on its certified Health IT Module(s) to incorporate these new versions is essential to support interoperability in the real world. Updated versions of standards reflect insights gained from real-world implementation and use. They also reflect industry stakeholders' interests to improve the capacity, capability, and clarity of such standards to meet new, innovative business needs, which earlier standards versions cannot support. Therefore, as part of the real world testing Condition of Certification, we propose a Maintenance of Certification flexibility that we refer to as the Standards Version Advancement Process. The Standards Version Advancement Process would permit health IT developers to voluntarily use in their certified Health IT Modules newer versions of adopted standards so long as certain conditions are met, not limited to but notably including successful real world testing of the Health IT Module using the new version(s).

We propose to establish the Standards Version Advancement Processnot only to meet the Cures Act's goals for interoperability, but also in response to the continuous stakeholder feedback that ONC has received through prior rulemakings and engagements, which requested that ONC establish a predictable and timely approach within the Program to keep pace with the industry's standards development efforts. Rulemaking has not kept up with the pace of standards development and deployment in the health care market. There is no better evidence of this reality than by example from our 2015 Edition rulemaking finalized approximately three years ago and before the Cures Act added Conditions and Maintenance of Certification provisions to the PHSA. Two version updates of the National Health Care Survey standard (versions 1.1 and 1.2) have been issued since we adopted version 1.0 in the 2015 Edition final rule (October 16, 2015). Health IT developer and health care provider compliance and use of these versions has and will be necessary for submission to Centers for Disease Control and Prevention (CDC) even though the certification criterion adopted in § 170.315(f)(7) continues to require conformance to version 1.0. Similarly, many other adopted standards have seen multiple newer versions introduced to the market since we issued the 2015 Edition final rule, such as for eCQM reporting or e-prescribing. The proposed Standards

[96] We note that standards development organizations and consensus standards bodies use various nomenclature, such as ''versions,'' to identify updates to standards and implementation specifications.

Version Advancement Process flexibility gives health IT developers the option to avoid such unnecessary costs and can help reduce market confusion by enabling certified Health IT Modules keep pace with standards advancement and market needs including but not limited to those related to emerging public health concerns.

We have also been informed by stakeholders that, in other cases, ONC's inability to more nimbly identify and incorporate newer versions to standards and implementation specifications that were already adopted by the Secretary into the Program has perversely impacted standards developing organization (SDO) processes. Although SDOs can rapidly iterate version updates to standards and implementation specifications to address ambiguities and implementation challenges reported from the field and to particularly address matters that adversely impact interoperability, the lack of a clear path for that work effort to be timely realized as part of the Program's certification requirements has had a chilling effect on the pace of change. It can also affect the willingness of volunteers at these SDOs to devote their time to make updates that would be outdated by the time ONC goes through a rulemaking, which can be years. Stakeholders have indicated that certified health IT developers, customers and users of certified health IT, and the SDO industry have been technologically restricted and innovation-stunted as a result of our prior regulatory approach, which focused on certification assuring compliance only to the version of a standard adopted in regulation and did not provide an avenue for the Program to accommodate iterative updates to standards during the time between rulemakings. With the passage of the ''maintenance of certification'' provision in § 4002 of the Cures Act, we believe the approach proposed here is in line with our new statutory authority regarding Conditions of Certification and Maintenance of Certification and would better and more timely support market demands for widespread interoperability.

In supporting more rapid advancement of interoperability, we believe the proposed Standards Version Advancement Process approach will benefit patient care, improve competition, and spur additional engagement in standards development. To this point, currently, if the USCDI v1 were adopted as currently proposed in § 170.213 and then needed to be updated to add just one data class or data element (*e.g.,* a new demographic element), we would need to initiate notice and comment rulemaking to incorporate that USCDI version change into the Program. Likewise, similar updates to standards included in our 2015 Edition final rule are made annually (or more frequently) by SDOs. In order to attempt to keep pace with such updates, which are published at different times of the year, ONC would need to continuously engage in rulemaking cycles, perhaps even more than once per year. We believe that the proposed Standards Version Advancement Process would allow for more advanced versions of standards and implementation specifications to be approved for use under the Program in a more timely and flexible manner that helps to ease the concerns stakeholders have reported. Stakeholder input throughout the Program's existence has informed ONC that updating large groupings of standards' versions while also adopting new standards through rulemakings that only occur about once every three years can create an artificial market impact in a number of ways. Such ''all-in-one'' updates affect all health IT developers and the vast majority of health care providers at the same time across all sectors rather than enabling a more incremental and market-based upgrade cycle in response to interoperability, business, and clinical needs.

The Standards Version Advancement Process and corresponding proposed revisions to §§ 170.550 and 170.555 would introduce two types of administrative flexibility for health IT developers participating in the Program. First, for those health IT developers with an existing certified Health IT Module, the Health IT Modules would be permitted to be upgraded (in the course of ongoing maintenance) to a new version of an adopted standard within the scope of the certification (without having to retest or recertify) so long as such version was approved by the National Coordinator for use in certification through the Standards Version Advancement Process. Second, for those health IT developers seeking to have a Health IT Module's initial certificate issued, the Health IT Module would be permitted to be presented for certification to a new version of an adopted standard so long as such version was approved by the National Coordinator through the Standards Version Advancement Process. This policy flexibility is similar to the flexibility we introduced several years ago for ''minimum standards'' code sets, but we would require ONC–ACBs to offer certification under the Standards Version Advancement Process to National-Coordinator-approved newer versions of all standards to which Real World Testing requirements apply.[97]

In order to ensure equitable treatment under the Program and in order for ONC to maintain the Program's overall integrity, each developer that chooses to leverage the proposed Standards Version Advancement Process Maintenance of Certification Program flexibilities would need to satisfy the following.

Health IT Developers Updating Already Certified Health IT

In instances where a health IT developer has certified a Health IT Module, including but not limited to instances where its customers are already using the certified Health IT Module, if the developer intends to update pursuant to the Standards Version Advancement Process election, the developer would be required to provide advance notice to all affected customers and its ONC–ACB: (a) Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator through the Standards Version Advancement Process; (b) the developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world; and (c) whether the developer intends to continue to support the certificate for the existing Health IT Module version for some period of time and how long, or if the existing version of the Health IT Module certified to prior version(s) of applicable standards will be deprecated (*e.g.,* that the developer will stop supporting the earlier version of the module and request to have the certificate withdrawn). The notice would be required to be provided sufficiently in advance of the developer establishing its planned timeframe for implementation of the upgrade to the more advanced standard(s) version(s) in order to offer customers reasonable opportunity to ask questions and plan for the update. We request public comment on the minimum time prior to an anticipated implementation of an updated standard or implementation

[97] For purposes of clarity, we note that the Standards Version Advancement Process would not affect the established minimum standards code sets flexibility. Consistent with § 170.555, under the Program, health IT could continue to be certified or upgraded to a newer version of identified minimum standards code sets (*see* 80 FR 62612) than even the most recent one the National Coordinator had approved for use in the Program via the Standards Version Advancement Process unless the Secretary prohibits the use of the newer version for certification.

specification version update that should be considered reasonable for purposes of allowing customers, especially health care providers using the Health IT Module in their health care delivery operations, to adequately plan for potential implications of the update for their operations and their exchange relationships. We would also be interested to know if commenters believe that there are specific certification criteria, standards, characteristics of the certified Health IT Module or its implementation (such as locally hosted by the customer using it versus software-as-a-service type of implementation), or specific types or characteristics of customers that could affect the minimum advance notice that should be considered reasonable across variations in these factors.

We anticipate providing ONC–ACBs (and/or health IT developers) with a means to attribute this updated information to the listings on the CHPL for the Health IT Modules the ONC–ACB has certified, and propose to require in the Principles of Proper Conduct for ONC–ACBs that they are ultimately responsible for this information being made publicly available on the CHPL. We request public comment on any additional information about updated standards versions that may be beneficial to have listed with certified Health IT Modules on the CHPL.

We clarify that a health IT developer would be able to choose which of the updated standards versions approved by the National Coordinator for use in certification through the Standards Version Advancement Process the developer seeks to include in its updated certified Health IT Module and would be able to do so on an itemized basis. In other words, if the National Coordinator were to approve for use through the Standards Version Advancement Process several different new versions of adopted standards that affected different certification criteria within the scope of a certified Health IT Module, the developer would be able to just update one certification criterion to one or more of the applicable new standards and would not have to update its Health IT Module to all of the National Coordinator-approved new versions all at once in order to be able to take advantage of this proposed flexibility.

Health IT Developers Presenting a New Health IT Module for Certification and Leveraging the Standards Version Advancement Process

In instances where a health IT developer presents a Health IT Module for certification for which no prior certificate can serve as the basis for using the Standards Version Advancement Process, we propose that the health IT developer would be permitted to use and implement any and all of the newer versions of adopted standards the National Coordinator approves through the Standards Version Advancement Process. We have implemented this proposed policy through necessary adjustments to the way in which ONC–ACBs process certifications in § 170.550. We recognize that this proposed flexibility reflects certain programmatic and policy trade-offs. On one hand, a health IT developer would be permitted to use the most recent version of standards approved by the National Coordinator instead of having to build in potentially ''outdated'' standards just to get certified. On the other hand, the Program's testing infrastructure (which is now inclusive of government-developed and non-government-developed tools) may experience certain lag times in terms of when updated test tools to support the approved version advancements would be available to test Health IT Modules for certification purposes. As a result, we propose to provide the ability for ONC–ACBs to accept a developer self-declaration of conformity as to the use, implementation, and conformance to a newer version of a standard (including but not limited to implementation specifications) as sufficient demonstration of conformance in circumstances where the National Coordinator has approved a version update of a standard for use in certification through the Standards Version Advancement Process but an associated testing tool is not yet updated to test to the newer version. Again, we clarify that a health IT developer would be able to choose which National Coordinator-approved standard version(s) it seeks to include in a new or updated certified Health IT Module and would be able to do so on an itemized basis.

On balance, we believe that this programmatic flexibility and the potential interoperability improvements from the use of newer versions of standards outweighs the subsequent oversight challenges. Moreover, these oversight challenges can be mitigated by the Standards Version Advancement Process itself (*i.e.,* the National Coordinator not approving a new version if the Program or industry is not ready) and the corresponding Conditions of Certification that continue with the use of National Coordinator-approved new versions of adopted standards. We also believe that this approach will continue to hold developers accountable for, and shift the focus of Health IT Module performance demonstration to, real world testing for interoperability for deployed Health IT Modules. As described above, we understand the limitations of test methods used prior to certification and further emphasize the importance of continued conformance of Health IT Modules in the field. However, we request comment on specific Program impacts we should consider.

General Requirements Associated With Health IT Modules Certified Using the Standards Version Advancement Process

In all cases, regardless of whether a health IT developer is updating an existing certified Health IT Module or presenting a new Health IT Module for certification to new versions of adopted standards approved by the National Coordinator through the Standards Version Advancement Process, it would need to adhere to the following once it elects to takes advantage of this proposed flexibility:

- The developer would need to ensure its mandatory disclosures in § 170.523(k)(1) appropriately reflect its use of any National Coordinator-approved newer versions of standards.
- The developer would need to address and adhere to all Conditions of Certification and Maintenance of Certification requirements proposed that are otherwise be applicable to its certified Health IT Modules regardless of whether those Health IT Modules were certified to the exact same versions of adopted standards that are listed in the text of 45 CFR part 170 or National Coordinator-approved newer version(s) of the standard(s). For instance, the developer would need to ensure that its real world testing plan and performance included the National Coordinator-approved standards versions to which it is claiming conformance.

In terms of compliance with the real world testing Condition and Maintenance of Certification requirements, the attestations Condition and Maintenance of Certification requirements proposed in § 170.406, and for the purposes of ONC–ACB surveillance, we note that health IT developers would be accountable for maintaining all applicable certified Health IT Modules in accordance with approved versions of standards and implementation specifications that they voluntarily elect to use in their certified health IT. If, at any point after initial certification or updated certification for a Health IT Module using the National Coordinator approved advanced versions of standards or implementation specifications, real world testing results do not demonstrate the Health IT Module's conformance to each applicable certification criterion had been achieved and maintained using the National Coordinator approved advanced version update of any applicable standard(s) and implementation specification(s), then the developer would not be allowed to claim or characterize the Health IT Module as conformant to the criterion using such standard version, and the standard or implementation specification version could not be indicated in the health IT Module's CHPL record as supported by any version release of the Health IT Module, until such time as they could demonstrate through ONC–ATL or results of real world testing that they had successfully upgraded the Health IT Module to fully conform to applicable certification criteria while incorporating the more advanced version of the standard. Non-conformities associated with the use of new versions of National Coordinator-approved standards would be found and enforced through the same Program rules just like they would be for non-conformities with the versions of adopted standards that are codified in regulation text. Further, we remind health IT developers that they would be required to make an attestation to their real world testing results, including (though not limited to) those that would be used to support use of new versions of National Coordinator-approved standards.

Advanced Version Approval Approach

Once a standard has been adopted for use in the Program through notice and comment rulemaking, ONC would undertake an annual, open and transparent process, including opportunity for public comment, to timely ascertain whether a more recent version of that standard or implementation specification should be approved for developers' voluntary use. ONC would identify updated versions of previously adopted standards and implementation specifications based on our own monitoring of market trends and interoperability needs, as well as input received from external stakeholders. Such external input may include, but would not be limited to, recommendations made by the Health Information Technology Advisory Committee as well as input received from SDOs.

ONC expects to use an expanded section of the Interoperability Standards Advisory (ISA) web platform to facilitate the public transparency and engagement process. At a particular time of the year (*e.g.,* early fall), ONC would post a list of new versions of adopted standards and implementation specifications that appear timely and appropriate for use within the Program (for the subsequent calendar year) along with accompanying descriptive context (*e.g.,* the types/nature of updates in the new version of a standard). ONC would then widely communicate to all members of the public that the list was available and make a general solicitation of comments to any and all interested parties for a period of 30 to 60 days. We would generally expect to receive comments on a range of issues related to the version of the standard under consideration, including its availability, testing tools, maturity, implementation burden, and overall impact on interoperability. Health IT developers, health information networks (HINs), and the health care organizations that purchase and use health IT are already familiar with the process of commenting through our existing ISA resource and we believe this process is well suited to support widespread engagement by all stakeholders. Similar to the ISA, we would expect to be open to receiving comments on newer versions of adopted standards throughout the year leading up to the formal comment period.

Once the formal comment period closes, ONC would review the comments and consider the potential impacts of a new version an adopted standard or implementation specification. We anticipate approving newer versions of adopted standards and implementation specifications based on several interdependent Program and market factors, such as its ability to enhance interoperability and overall compatibility with other adopted versions, how burdensome it would be to update to the newer version and the scope and scale of the changes, whether the new version would be required for reporting by a corresponding program (*e.g.,* CMS or CDC), the availability of test tools for the new version, and the new version's relationship to other adopted standards and any dependencies. Upon concluding our review and analysis, ONC would publish in this new ISA section a final list of National Coordinator-approved advanced versions that health IT developers could electively use consistent with the Standards Version Advancement Process.

Within this proposed approach, we expect that when it comes to a standard, the National Coordinator would identify version updates to an adopted standard consistent with that standard's name and version track. This method would provide long-term consistency for health IT developers in terms of the overall technical conformance requirements on which they will be focused.

With respect to adopted implementation specifications, we believe that more flexibility about the precise name and version track identifiers would be warranted given that implementation specifications are developed by market-driven industry consortia (*e.g.,* Argonaut project and Direct project stakeholders) as well as traditional SDOs. Similarly, authors of implementation specifications sometimes develop supplemental documents to the "parent" implementation specification or split the implementation specification to form newly titled materials. In any of these cases, the resulting implementation specification may—on its face—initially appear to bear no relation to a previously adopted implementation specification because of changes to its title, version naming, or numbering presentation. In reality, in many of these cases, the implementation specification retains substantially the same purpose(s) and thus represents a versioning update rather than amounting to a novel specification. Accordingly, regardless of its title and author, the National Coordinator would take into account whether any "new" implementation specification under consideration is more accurately characterized as novel to the Program or instead is a derivative work that is substantially a more advanced version of a previously adopted implementation specification(s). Stakeholders would also be able to comment on the same during the advanced version approval process described here.

The public listing of these National Coordinator determinations to approve version updates to already adopted standards and implementation specifications would serve as the single, comprehensive, and authoritative index of the versions of adopted standards and implementation specifications available for use under the Program. We note, however, that certain Program administration steps would need to occur (such as ONC–ACBs expanding the scope of their accreditations) after the National Coordinator has approved newer versions of adopted standards. As a result, there would likely be a temporary delay between the National Coordinator's approval decision and when certification to new standards versions under the Program would start.

We welcome comments on any and all aspects of our proposed standards version approval process as an option available to developers through maintenance requirements as part of the real world testing Condition and Maintenance of Certification. This includes all aspects of our described approach to standards and implementation specification advanced version approval processes. We also invite comments on our proposal to allow in conjunction with this maintenance flexibility the opportunity for developers to elect to present health IT for initial testing and certification either to more advanced versions or the prior versions included in regulatory text as of the date the technology is presented.

Principle of Proper Conduct for ONC–ACB for All Real World Testing Proposals

We propose to include a new Principle of Proper Conduct for ONC–ACBs in § 170.523(p) that would require ONC–ACBs to review and confirm that applicable health IT developers submit real world testing plans and results in accordance with our proposals. We expect that ONC–ACBs would review the plans for completeness. Once completeness is confirmed, ONC–ACBs would provide the plans to ONC by December 15 and results to ONC by April 1. The December 15 date is the same date as the health IT developer requirement for submission of the real world testing plan. For purposes of the Program, this treats both regulated entities equally and permits them to work out a process that ensures all real world testing plans are submitted to the CHPL by December 15. For example, a health IT developer that is confident in its plan and does not anticipate any further certification, may submit its plan in July of the preceding year.

The submission of results, however, does not present the same dynamic of the potential need to work together to ensure the plan is complete. As such, we have proposed different dates. We would expect the developers to submit their results by January 31. We believe this would provide sufficient time for ONC–ACBs to review all plans and post them to the CHPL by April 1, including notifying ONC when the results were not in compliance with requirements. ONC would make both the plans and results publicly available via the CHPL. We note that ONC–ACBs will continue to be required to perform in-the-field surveillance of certified Health IT Modules and results of real world testing could be considered information to inform ONC–ACB surveillance activities.

Because we are proposing to allow health IT developers to implement National Coordinator-approved advanced versions of standards and implementation specifications in certified Health IT Modules through a developer self-declaration of conformity presented for certification if an associated testing tool is not yet updated to test to the newer version for the standards and implementation specification version updates they have chosen to use in the Program, we propose two requirements to ensure the public and ONC–ACBs have knowledge of the version of a standard that certified health IT meets. First, we propose to revise the Principle of Proper Conduct in § 170.523(m) to require ONC–ACBs to collect, no less than quarterly, all version updates made to standards successfully included in certified health IT per the requirements within the real world testing Condition of Certification Standards Version Advancement Process. This would ensure that ONC–ACBs are aware of the version of a standard that certified health IT meets for the purposes of surveillance and Program administration. Second, we propose (as discussed above), that a developer that chooses to avail itself of the Standards Version Advancement Process flexibility must address in its real world testing plans and results submissions the timeline and rollout of applicable version updates for standards and implementation specifications. This addition to § 170.523(m) along with existing requirements for weekly ONC–ACB CHPL reporting to versions of standards per § 170.523(f)(1)(xvii) would allow for timely updates to Health IT Module certificate information in the CHPL. Together with the requirements (discussed above) for developers' communication with their current and potential customers, we intend to ensure that the public and end-users have transparency into planned and actual standards and implementation specifications updates for their certified health IT.

In complement to the above requirements to ensure transparency for the public and end users, we propose in § 170.523(t) a new Principle of Proper Conduct for ONC–ACBs requiring them to ensure that developers seeking to take advantage of the Standards Version Advancement Process flexibility in § 170.405(b)(5) comply with the applicable requirements, and that the ONC–ACB both retain records of the timing and content of developers' § 170.405(b)(5) notices and timely post each notice's content publicly on the CHPL attributed to the certified Health IT Modules to which it applies.

We seek comment on the proposed additions to the Principles of Proper Conduct for ONC–ACBs. More specifically, we seek comment on whether ONC–ACBs should be required to perform an evaluation beyond a completeness check for the real world testing plans and results and the value versus the burden of such an endeavor.

6. Attestations

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, provide to the Secretary an attestation to all the Conditions of Certification specified in the Cures Act, except for the ''EHR reporting criteria submission'' Condition of Certification. We propose to implement the Cures Act ''attestations'' requirements Condition of Certification in § 170.406. We also propose that, as part of the implementation of this statutory provision, health IT developers would attest, as applicable, to compliance with the Conditions and Maintenance of Certification requirements described in this section of the preamble and proposed in §§ 170.401 through 170.405.

We propose that, as a Maintenance of Certification requirement for the ''attestations'' Condition of Certification, health IT developers must submit their attestations every 6 months (*i.e.,* semiannually). We believe this would provide an appropriate ''attestation period'' to base any enforcement actions, such as by ONC under the Program or by the Office of the Inspector General under its Cures Act authority. We also believe this 6-month attestation period properly balances the need to support appropriate enforcement actions with the attestation burden placed on developers. We will determine when the first attestation will be due depending on when the final rule is published. We require attestations to be due twice a year, likely in the middle and end of the calendar year.

The process we plan to implement for providing attestations should minimize burden on health IT developers. First, we propose to provide a 14-day attestation period twice a year. For health IT developers presenting health IT for certification for the first time under the Program, we propose that they would be required to submit an attestation at the time of certification and then also comply with the semiannual attestation periods. Second, we would publicize and prompt developers to complete their attestation during the required attestation periods. Third, we propose to provide a method for health IT developers to indicate their compliance, non-compliance with, or the inapplicability of each Condition and Maintenance of Certification requirement as it applies to all of their health IT certified under the Program for each attestation period. Last, we propose to provide health IT developers the flexibility to specify non-compliance per certified Health IT Module, if necessary. We note, however, that any non-compliance with the proposed Conditions and Maintenance of Certification requirements, including the ''attestations'' Conditions and Maintenance of Certification requirements, would be subject to ONC direct review, corrective action, and enforcement procedures under the Program. We refer readers to section VII.D of this preamble for discussion of proposed ONC direct review, corrective action, and enforcement procedures for the Conditions and Maintenance of Certification requirements under the Program.

We propose that attestations would be submitted to ONC–ACBs on behalf of ONC and the Secretary. We propose that ONC–ACBs would have two responsibilities related to attestations. One responsibility we propose in § 170.523(q) is that an ONC–ACB must review and submit the health IT developers' attestations to ONC. ONC would then make the attestations publicly available through the CHPL. The other responsibility we propose in § 170.550(l) is that before issuing a certification, an ONC–ACB would need to ensure that the health IT developer of the Health IT Module has met its responsibilities related to the Conditions and Maintenance of Certification requirements as solely evidenced by its attestation. For example, if a health IT developer with an active certification under the Program indicated non-compliant designations in their attestation but is already participating in a corrective action plan under ONC direct review to resolve the non-compliance, certification would be able to proceed while the issue is being resolved.

We welcome comments on the proposed attestations Condition and Maintenance of Certification requirements, including the appropriate frequency and timing of attestations. We also welcome comments on the proposed responsibilities for ONC–ACBs related to the attestations of Condition and Maintenance of Certification requirements.

7. EHR Reporting Criteria Submission

The Cures Act specifies that health IT developers be required, as a Condition and Maintenance of Certification under the Program, to submit reporting criteria on certified health IT in accordance with the EHR reporting program established under section 3009A of the PHSA, as added by the Cures Act. We have not yet established an EHR reporting program. Once ONC establishes such program, we will undertake future rulemaking to propose and implement the associated Condition and Maintenance of Certification requirement(s) for health IT developers.

C. Compliance

The proposed Maintenance of Certification requirements discussed above do not necessarily define all the outcomes necessary to meet the Conditions of Certification. Rather, they provide preliminary or baseline evidence toward measuring whether a Condition is being met. Thus, ONC could determine that a Condition of Certification is not being met through reasons other than the Maintenance of Certification requirements. For example, meeting the proposed Maintenance of Certification requirement that requires a health IT developer to not establish or enforce any contract or agreement that contravenes the Communications Condition of Certification does not excuse a health IT developer from meeting all the requirements specified in the proposed Communications Condition of Certification. This is analogous to clarifications ONC has previously provided about certification criteria requirements whereby testing prior to certification sometimes only tests a subset of the full criterion's intended functions and scope. However, for compliance and surveillance purposes, we have stated that ONC and its ONC–ACBs will examine whether the certified health IT meets the full scope of the certification criterion rather than the subset of functions it was tested against (80 FR 62709–10).

D. Enforcement

The Cures Act affirms ONC's role in using certification to improve health IT's capabilities for the access, use, and exchange of electronic health information. The Cures Act provides this affirmation through expanded certification authority for ONC to establish Conditions and Maintenance of Certification requirements for health IT developers that go beyond the certified health IT itself. The new Conditions and Maintenance of Certification provisions in section 4002 of the Cures Act focus on the actions and business practices of health IT developers (*e.g.,* information blocking and appropriate access, use, and exchange of electronic health information) as well as technical interoperability of health IT (*e.g.,* APIs and real world testing). Furthermore and equally important, section 4002 of the Cures Act provides that the Secretary of HHS may encourage compliance with the Conditions and Maintenance of Certification requirements and take action to discourage noncompliance. As discussed in the 2015 Edition final rule, ONC is not limited to enforcing Program compliance solely through those requirements expressed in certification criteria adopted under the Program (80 FR 62710; see also 81 FR 72412). Certification under the Program also relies on a health IT developer's compliance with Program requirements that ensure the basic integrity and effectiveness of the Program, which is further stressed through the addition of the Conditions and Maintenance of Certification requirements in the Cures Act (referred to jointly as the ''Conditions and Maintenance of Certification'' in this section of the preamble).

Given these considerations, we propose a general enforcement approach outlining a corrective action process for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement has not been or is not being met by a health IT developer under the Program, including the requirement for a health IT developer to attest to meeting the Conditions and Maintenance of Certification. Table 2 below provides an overview of the proposed approach to ONC enforcement of the Conditions and Maintenance of Certification. We provide more specific proposals following Table 2.

TABLE 2—PROPOSED APPROACH FOR ENFORCEMENT OF THE CONDITIONS AND MAINTENANCE OF CERTIFICATION

Proposed regulatory text	Condition of certification	Opportunity for developer to take corrective action	Consequences of not taking appropriate corrective action	Opportunity for developer to appeal ONC determination to terminate or ban
§ 170.401	Information Blocking	Yes	Certification ban of all of a developer's certified Health IT Modules.	Yes.
§ 170.402	Assurances.			
§ 170.403	Communications.		ONC may also consider termination of Health IT Module certificates if there is a nexus between the developer's practices and a certified Health IT Module.	
§ 170.404	APIs.			
§ 170.405	Real World Testing.			
§ 170.406	Attestations.			

1. ONC Direct Review of the Conditions and Maintenance of Certification Requirements

We propose to utilize the processes previously established for ONC direct review of certified health IT in the EOA final rule (81 FR 72404) and codified in §§ 170.580 and 170.581 for the enforcement of the Conditions and Maintenance of Certification. We propose this approach for multiple reasons. First, these processes were established to address non-conformities with Program requirements. Conditions and Maintenance of Certification are proposed to be adopted as Program requirements and, as such, any noncompliance with the Conditions and Maintenance of Certification would constitute a Program non-conformity. Second, health IT developers are familiar with the ONC direct review provisions as they were established in October 2016. Third, §§ 170.580 and 170.581 provide thorough and transparent processes for working with health IT developers through notice and corrective action to remedy Program non-conformities. Last, the direct review framework provides equitable opportunities for health IT developers to respond to ONC actions and appeal certain ONC determinations.

2. Review and Enforcement Only by ONC

We propose to retain use of the term ''direct review'' as previously adopted in the EOA final rule to continue to distinguish actions ONC takes to directly review certified health IT or health IT developers' actions in comparison to an ONC–ACB's review of certified health IT under surveillance. We propose, however, that ONC would be the sole party responsible for enforcing compliance with the Conditions and Maintenance of Certification. The Conditions and Maintenance of Certification focus on health IT developer behavior and actions in addition to the certified Health IT Module. ONC is more familiar with the behavioral requirements based on its expertise and experience. Conversely, ONC–ACBs are generally more suited, based on their accreditation and current responsibilities, to address non-conformities with technical and other Program requirements. ONC also has the necessary resources and the ability to coordinate with other agencies to enforce the Conditions and Maintenance of Certification, such as with the ''information blocking'' Condition of Certification (proposed § 170.401). Further, ONC enforcement would provide more predictability and consistency, which would likely benefit stakeholders in matters related to API fees and information blocking. We do, however, discuss below the scope of ONC–ACB surveillance as it relates to ONC's proposed enforcement of the Conditions and Maintenance of Certification.

3. Review Processes

We propose to substantially adopt the processes as they are currently codified in §§ 170.580 and 170.581 for ONC's review and enforcement of the Conditions and Maintenance of Certification, but propose certain revisions and additions to the processes to properly incorporate the proposed Conditions and Maintenance of Certification and effectuate Congressional intent. These revisions and additions include renaming and restructuring headings for clarity, which we do not discuss below.

a. Initiating Review and Health IT Developer Notice

We propose to fully incorporate the review of the Conditions and Maintenance of Certification into the provisions of § 170.580(a) and (b). We propose in § 170.580(a)(iii) that if ONC has a reasonable belief that a health IT developer has not complied with a Condition of Certification, then it *may* initiate direct review. Similarly, we propose in § 170.580(b)(1) and (2) that ONC may issue the health IT developer a notice of potential non-conformity or notice of non-conformity and provide the health IT developer an opportunity to respond with an explanation and written documentation, including any information ONC requests. These processes, including relevant timeframes, are specified in § 170.580(b).

i. Complaint Resolution

We note and recommend that customers and end-users first work with their health IT developers to resolve any issues of potential non-compliance with the Conditions and Maintenance of Certification as prior Program experience has shown that many issues can be resolved at this step. If the issue cannot be resolved, we then recommend the end-user contact the ONC–ACB. However, as discussed above and in section VII.D.5 below, the ONC–ACB purview for certified health IT generally applies to certified capabilities and limited requirements of developer business practices. If neither of these pathways resolves the issue, end-users may provide feedback to ONC via the Health IT Feedback Form.[98]

ii. Method of Correspondence With Health IT Developers

Section 170.505 states that correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. In the EOA final rule, we signaled our intent to send notices of potential non-conformity, non-conformity, suspension, proposed termination, and termination via certified mail (81 FR 72429). However, in accordance with § 170.505, we propose that email should be the default mode of correspondence for direct review of non-compliance with the Conditions and Maintenance of Certification.

[98] *https://www.healthit.gov/form/healthit-feedback-form.*

Under the EOA final rule, ONC can initiate direct review of certified health IT in limited circumstances, namely when there is a reasonable belief that the certified health IT may be causing or contributing to serious risks to public health or safety or suspected non-conformities present practical challenges that may prevent an ONC–ACB from effectively investigating or responding to the suspected non-conformity. In contrast, we propose in this proposed rule to enable ONC to initiate direct review to address a health IT developer's conduct under the Conditions and Maintenance of Certification requirements in addition to non-conformities in certified health IT. This proposal would create an expanded set of circumstances for ONC to conduct direct review. Accordingly, the type and extent of review by ONC could vary significantly based on the complexity and severity of each fact pattern. For instance, ONC may be able to address certain non-conformities under the Conditions and Maintenance of Certification quickly and with minimal effort (*e.g.,* failure to make public a documentation hyperlink), while others may be more complex and require additional time and effort (*e.g.,* violation of API fee prohibitions). Considering this wide range of potential non-conformities under the Conditions and Maintenance of Certification, we believe it is appropriate for ONC to retain discretion to decide, on a case-by-case basis, when to go beyond the provisions of § 170.505 in providing notices and correspondence for non-compliance with the Conditions and Maintenance of Certification.

We solicit comment on the nature and types of non-conformities with the Conditions and Maintenance of Certification requirements that ONC should consider in determining the method of correspondence. We also solicit comment on whether the type of notice should affect the method of correspondence and whether certain types of notices under direct review should be considered more critical than others, thus requiring a specific method of correspondence.

b. Relationship With ONC–ACBs and ONC–ATLs

Section 170.580(a)(3) outlines ONC direct review in relation to the roles of ONC–ACBs and ONC–ATLs, which we propose to revise to incorporate Conditions and Maintenance of Certification. We note that we provide situational examples below in section VII.D.5 ''Effect on Existing Program Requirements and Processes'' regarding ONC direct review and the role of an ONC–ACB. As finalized in the EOA final rule and per § 170.580(a)(3)(v), we remind readers that ONC may refer the applicable part of its review of certified health IT to the relevant ONC–ACB(s) if ONC determines this would serve the effective administration or oversight of the Program (81 FR 72427–72428).

c. Records Access

We propose to revise § 170.580(b)(3) to ensure that ONC, or third parties acting on its behalf, has access to the information necessary to enforce the Conditions and Maintenance of Certification. As specified in § 170.580(b)(1)(ii)(A)(*2*), (b)(2)(ii)(A)(*2*) and (b)(3), in response to a notice of potential non-conformity or notice of non-conformity, ONC must be granted access to, and have the ability to share within HHS, with other federal agencies, and with appropriate entities, all of a health IT developers' records and technology related to the development, testing, certification, implementation, maintenance, and use of a health IT developers' certified health IT; and any complaint records related to the certified health IT. ''Complaint records'' include, but are not limited to issue logs and help desk tickets (81 FR 72431). We propose to supplement these requirements with a requirement that a health IT developer make available to ONC, and third parties acting on its behalf, records related to marketing and distribution, communications, contracts, and any other information relevant to compliance with any of the Conditions and Maintenance of Certification or other Program requirements. This information would assist in reviewing allegations that a health IT developer violated, for example, the ''prohibit and restrict communications'' Condition of Certification. Further, it is possible that multiple Conditions and Maintenance of Certification may be implicated under a review, and thus ONC believes it is appropriate to require a developer make available to ONC *all* records and other relevant information concerning all the Conditions and Maintenance of Certification and Program requirements to which it and its Health IT Modules are subject.

If ONC determined that a health IT developer was not cooperative with the fact-finding process, we propose ONC would have the ability to issue a certification ban and/or terminate a certificate (*see* proposed § 170.581 discussed below and § 170.580(f)(1)(iii)(A)(*1*)).

We understand that health IT developers may have concerns regarding the disclosure of proprietary, trade secret, competitively sensitive, or other confidential information. As we stated in the EOA final rule (81 FR 72429), ONC would implement appropriate safeguards to ensure, to the extent permissible with federal law, that any proprietary business information or trade secrets ONC may encounter by accessing the health IT developer's records, other information, or technology, would be kept confidential by ONC or any third parties working on behalf of ONC. However, a health IT developer would not be able to avoid providing ONC access to relevant records by asserting that such access would require it to disclose trade secrets or other proprietary or confidential information. Therefore, health IT developers must clearly mark, as described in HHS Freedom of Information Act regulations at 45 CFR 5.65(c), any information they regard as trade secret or confidential commercial or financial information which they seek to keep confidential prior to disclosing the information to ONC or any third party working on behalf of ONC.

d. Corrective Action

We propose that if ONC determines that a health IT developer is noncompliant with a Condition of Certification (*i.e.,* a non-conformity), ONC would work with the health IT developer to establish a corrective action plan (CAP) to remedy the issue through the processes specified in § 170.580(b)(2)(ii)(A)(*4*) and (c). We note that a health IT developer may be in noncompliance with more than one Condition of Certification. In such cases, ONC will follow the proposed compliance enforcement process for each Condition of Certification accordingly, but may also require the health IT developer to address all violations in one CAP for efficiency of process. We also propose, as we currently do with CAPs for certified health IT, to list health IT developers under a CAP on ONC's website.

e. Certification Ban and Termination

We propose in § 170.581 that if a health IT developer under ONC direct review for non-compliance with a Condition of Certification failed to work with ONC or was otherwise noncompliant with the requirements of the CAP and/or CAP process, ONC could issue a certification ban for the health IT developer (and its subsidiaries and successors). A certification ban, as it currently does for other matters under § 170.581, would prohibit prospective certification activity by the health IT developer.

ONC would also consider termination [99] of the certificate(s) of the affected Health IT Module(s) should the health IT developer fail to work with ONC or is otherwise noncompliant with the requirements of the CAP and/or CAP process (*see* proposed § 170.580(f)(1)(iii)). ONC may consider termination if there is a nexus between the developer's actions or business practices and certified Health IT Module(s) (*see* proposed § 170.580(f)(1)(iii)). For example, ONC may determine that a health IT developer is violating a Condition of Certification due to a clause in its contracts that prevents its users from sharing or discussing technological impediments to information exchange. In this example, the health IT developer's conduct would violate the ''prohibiting or restricting communication'' Condition of Certification proposed in § 170.403. If the same conduct were also found to impair the functionality of the certified Health IT Module (such as by preventing the proper use of certified capabilities for the exchange of EHI), ONC may determine that a nexus exists between the developer's business practices and the functionality of the certified Health IT Module, and may consider termination of the certificates of that particular Health IT Module under the proposed approach.

We propose this approach, which allows ONC to initiate a certification ban and/or certificate termination under certain circumstances, to ensure that health IT developers are acting in accordance with the Conditions and Maintenance of Certification. However, we stress that our first and foremost priority is to work with health IT developers to remedy any noncompliance with Conditions and Maintenance of Certification through a corrective action process before taking further action. This emphasizes ONC's desire to promote and support health IT developer compliance with the Conditions and Maintenance of Certification and ensure that certified health IT is compliant with Program requirements in order to foster an environment where EHI is exchanged in an interoperable way.

ONC does not believe that noncompliance with a Condition of Certification should always result in the termination of the certificate of one or more of a developer's Health IT Modules for a few reasons. A violation of a Condition of Certification may relate solely to health IT developer business practices or actions that do not affect the Health IT Module's conformance to the requirements of the certification criteria. In this case, termination of the certification could unfairly and negatively affect a provider's ability to use the Health IT Module for participation in CMS programs that require certification because the Health IT Module itself is functioning in accordance with the technical requirements of its certificate.[100] As such, ONC would carefully consider on a case-by-case basis the appropriateness of termination of a Health IT Module's certification(s) based on the specific circumstances of the noncompliance with the Condition of Certification. The proposed enforcement approach balances the above stated goals and provides an outlined process that can be consistently followed.

In considering whether termination of a Health IT Module's certificate(s) and/or a certification ban is appropriate, ONC will consider factors including, but not limited to: Whether the health IT developer has previously been found in noncompliance with the Conditions and Maintenance of Certification or other Program requirements; the severity and pervasiveness of the noncompliance, including the effect of the noncompliance on widespread interoperability and health information exchange; the extent to which the health IT developer cooperates with ONC to review the noncompliance; the extent of potential negative impact on providers who may seek to use the certified health IT to participate in CMS programs; and whether termination and/or a certification ban is necessary to ensure the integrity of the certification process.

As under § 170.580(f)(2), ONC would provide notice of the termination to the health IT developer, including providing reasons for, and information supporting, the termination and instructions for appealing the termination. We propose to add similar notice provisions to § 170.581 for certification bans issued under ONC direct review for non-compliance with the Conditions and Maintenance of Certification, which would also include instructions for requesting reinstatement. In this regard, we propose to apply the current reinstatement procedures under § 170.581 to Conditions and Maintenance of Certification bans, but with an additional requirement that the health IT developer has resolved the non-compliance with the Condition of Certification. In sum, a health IT developer could seek ONC's approval to re-enter the Program and have the certification ban lifted if it demonstrates it has resolved the noncompliance with the Condition of Certification and ONC is satisfied that all affected customers have been provided appropriate remediation.

For clarity, a health IT developer would have an opportunity to appeal an ONC determination to issue a certification ban and/or termination IT resulting from a non-conformity with a Condition of Certification as discussed below and/or seek reinstatement in the Program and have the certification ban lifted. To note, we propose to make terminations effective consistent with current § 170.580(f)(2)(iii) and similarly for certification bans (*see* proposed § 170.581(c)). We seek comment on whether ONC should:

- Impose a minimum certification ban length before a health IT developer can request ONC remove the ban for health IT developers who are noncompliant with a Condition of Certification more than once (*e.g.,* a minimum six months for two instances, a minimum of one year for three instances).
- Consider additional factors for a certification ban and/or the termination of a health IT developer's certified health IT resulting from a non-conformity with a Condition of Certification.

f. Appeal

We propose to provide a health IT developer an opportunity to appeal an ONC determination to issue a certification ban and/or termination resulting from a non-conformity with a Condition of Certification and would follow the processes specified in § 170.580(g). As such, we propose to revise § 170.580(g) to include ONC direct review of the Conditions and Maintenance of Certification.

g. Suspension

Section 170.580 includes a process for suspending the certification of a Health IT Module at any time if ONC has a reasonable belief that the certified health IT may present a serious risk to public health and safety. While this will

[99] As noted in the EOA final rule, ''termination'' means an ONC action to ''terminate'' or ''revoke'' the certification status of a Complete EHR or Health IT Module. (81 FR 72443).

[100] Note that, in this example, an ONC–ACB may investigate the technical functionalities of the Health IT Module against its certificate and perform surveillance under § 170.556 separate from ONC's process to enforce compliance with the Conditions of Certification. If under ONC–ACB surveillance, a health IT developer does not adequately or timely fulfill a corrective action plan, the ONC–ACB may suspend and withdraw the Health IT Module's certificate. The expectations of ONC–ACB duties as relates to ONC's enforcement of the conditions of certification are described further in the preamble.

remain the case for certified health IT under ONC direct review (*i.e.,* suspension of certification is always available under ONC direct review when the certified health IT presents a serious risk to public health and safety), we do not believe such circumstances would apply to noncompliance with the Conditions of Certification. Further, we believe the more streamlined processes proposed for addressing noncompliance with Conditions and Maintenance of Certification alleviates the need to proceed through a suspension process. Therefore, we do not propose to apply the suspension processes under § 170.580 to our review of the Conditions of Certification. We welcome comments on this proposal, including reasons for why we should apply suspension processes to the Conditions of Certification as part of a subsequent final rule.

h. Proposed Termination

Section 170.580 includes an intermediate step between a developer failing to take appropriate and timely corrective action and termination of a certified Health IT Module's certificate, called ''proposed termination'' (*see* § 170.580(e) and 81 FR 72437)). We propose to *not* include this step when a health IT developer fails to take appropriate and timely corrective action for noncompliance with a Condition of Certification. Rather, as discussed above, ONC may proceed directly to issuing a certification ban or notice of termination if it determines a certification ban and/or termination are appropriate per the considerations discussed above. The Conditions and Maintenance of Certification include requirements of developer business practices and actions for which, as previously discussed, noncompliance with the Conditions and Maintenance of Certification in these arenas are likely to undermine the integrity of the Program and impede widespread interoperability and information exchange. As such, ONC believes it is appropriate and consistent with the Cures Act to proceed immediately to a certification ban and/or termination of the affected certified Health IT Modules' certificates if a developer does not take appropriate and timely corrective action. A certification ban and/or termination are appropriate disincentives for noncompliance with the Conditions and Maintenance of Certification.

4. Public Listing of Certification Ban and Terminations

We propose to publicly list health IT developers and certified Health IT Modules on ONC's website that are subject to a certification ban and/or have been terminated, respectively, for noncompliance with a Condition of Certification or for reasons already specified in § 170.581. We currently take this same approach for health IT with terminated certifications (*see* 81 FR 72438). Public listing serves to discourage noncompliance with Conditions and Maintenance of Certification, other Program requirements, remediation of non-conformities, and cooperation with ONC and the ONC–ACBs. It also serves to provide notice to all ONC–ATLs, ONC–ACBs, public and private programs requiring the use of certified health IT, and consumers of certified health IT of the status of certified health IT and health IT developers operating under the Program.

We seek comment on this proposal, including input on the appropriate period of time to list health IT developers and affected certified Health IT Modules on healthit.gov. For example, if a developer sought and received reinstatement under the Program (and lifting of the certification ban), should the health IT developer no longer be listed on the ONC website? Alternatively, should we list health IT developers who have been subject to the certification ban under § 170.581 for a certain period of time beyond the active ban, including indefinitely (*e.g.,* with the timeframe when the ban was active)?

5. Effect on Existing Program Requirements and Processes

The Cures Act introduces new Conditions and Maintenance of Certification that encompass technical and functional requirements of health IT and new actions and business practice requirements for health IT developers, which ONC proposes to adopt in subpart D of Part 170. The pre-Cures Act structure and requirements of the Program provide processes to enforce compliance with technical and functional requirements of certified health IT, and to a more limited extent, requirements for the business practices of health IT developers (see, *e.g.,* 45 CFR 170.523(k)(1)) under subparts C (Certification Criteria for Health Information Technology) and E (ONC Health IT Certification Program) of Part 170. ONC–ACBs are required to perform surveillance on certified Health IT Modules and may investigate reported alleged non-conformities with Program requirements under subparts A, B, C, and E with the ultimate goal to work with the health IT developer to correct the non-conformity. Under certain situations, such as unsafe conditions or impediments to ONC–ACB oversight, ONC may directly review certified health IT to determine whether it conforms to the requirements of the Program (*see* § 170.580 and the EOA final rule at 81 FR 72404). These avenues for investigating non-conformities with certified Health IT Modules will continue to exist under the Program and generally focus on functionality and performance of certified health IT or more limited requirements of business practices of health IT developers found in subparts A, B, C and E of Part 170, respectively. Thus, there may be instances where one or more Conditions and Maintenance of Certification are not being or have not been met that also relate to certified Health IT Modules non-conformities under subparts A, B, C and E. Under these situations, ONC could in parallel implement both sets of processes—existing processes to investigate Health IT Module non-conformities and the proposed process to enforce compliance with the Conditions and Maintenance of Certification.

We again note that under the proposed enforcement approach, only ONC would have the ability to determine whether a Condition or Maintenance of Certification requirement per subpart D has been or is being met. We propose to delineate the scope of an ONC–ACB's requirements to perform surveillance on certified Health IT Modules as related only to the requirements of subparts A, B, C and E of Part 170. Table 3 below further illustrates the proposed difference in scope of review activities between ONC–ACBs and ONC. Given our proposed approach that would authorize solely ONC to determine whether a Condition or Maintenance of Certification requirement per subpart D has been or is being met, we propose to add a new Principle of Proper Conduct for ONC–ACBs in § 170.523(s) that would require ONC–ACBs to report to ONC, no later than a week after becoming aware, any information that could inform whether ONC should exercise direct review for noncompliance with a Condition of Certification or any matter within the scope of ONC direct review. We believe this is appropriate because ONC–ACBs receive complaints and other information about certified Health IT Modules through their own channels; as this information may relate to potential noncompliance with the Conditions and Maintenance of Certification or other matters within the scope of ONC direct review, ONC should be made aware of this information.

TABLE 3—SCOPE OF ONC–ACB SURVEILLANCE AND ONC DIRECT REVIEW FOR PROPOSED ENFORCEMENT APPROACH FOR CONDITIONS AND MAINTENANCE OF CERTIFICATION

Condition of certification	ONC–ACB purview for surveillance per 170.556	ONC purview for enforcement per 170.580 and 170.581
170.401: Information Blocking	Only as it relates to Subparts A, B, C and E of Part 170	All of 170.401.
170.402: Assurances	Only as it relates to Subparts A, B, C and E of Part 170, including the certification criterion in § 170.315(b)(10) "EHI export".	All of 170.402.
170.403: Communications	Only as it relates to Subparts A, B, C and E of Part 170	All of 170.403.
170.404: APIs	Only as it relates to Subparts A, B, C and E of Part 170, including the certification criterion in § 170.315(g)(10).	All of 170.404.
170.405: Real World Testing	Only as it relates to Subparts A, B, C and E of Part 170	All of 170.405.
170.406: Attestations	Only as it relates to Subparts A, B, C and E of Part 170	All of 170.406.

For example and further illustration purposes, ONC may receive a complaint of information blocking alleging that a health IT developer has limited the ability to receive secure Direct messages from users of a competing developer's EHR. The complaint alleges the certified health IT drops the incoming message without alerting the user that a message was ever received. ONC would consider the information blocking concerns (proposed § 170.401) as well as the potential safety concerns presented by dropped messages associated with certified functionality of the 2015 Edition "transitions of care" certification criterion (§ 170.315(b)(1)) and standards for the secure Direct messaging in its review. For the potential safety concerns, ONC would be exercising its authority to review certified health IT that may be causing or contributing to conditions that present a serious risk to public health or safety under § 170.580(a)(2)(i). In contrast, the ONC–ACB would not be responsible for reviewing the information blocking or safety concerns directly, but it *would* be responsible for assessing whether surveillance needs to be performed on the certified health IT for the functionality in the 2015 Edition "transitions of care" certification criterion (§ 170.315(b)(1)) and the 2015 Edition "Direct Project" certification criterion (§ 170.315(h)(1)), as these requirements are found within subpart C of Part 170 and could be implicated based on the complaint.

To provide another example, an ONC–ACB could receive complaints from users that a developer's certified health IT does not support the FHIR DSTU 2 standard and associated API resource collection in health (ARCH Version 1) as required in the proposed new 2015 Edition certification criterion § 170.315(g)(10) (proposed under subparts B and C).The respective ONC–ACB(s) responsible for the certification of the certified health IT could surveil this health IT under the requirements of § 170.556 (under subpart E). Additionally, ONC could follow the CAP process under § 170.580(c) to enforce the associated "API" Condition of Certification proposed in § 170.404(a)(2). During the course of the ONC–ACB surveillance, the ONC–ACB subsequently discovers the developer has implemented the FHIR DSTU 2 standard and associated resources in such as a way that the patient's historical medications are being accessed, but not the patient's current medications. The ONC–ACB would notify ONC of its findings as it relates to a Condition of Certification under subpart D and pursue its own corrective action process under the surveillance requirements of § 170.556. Once ONC receives information regarding the complaints from the ONC–ACB, we could consider the potential safety risks for providers using the developer's API to access new or referred patients' medical information for diagnostic and treatment purposes. In this example, ONC could review both the certified health IT and the developer action under § 170.580, which is proposed to be expanded to account for developer actions under the Conditions and Maintenance of Certification (*see* proposed § 170.580(a)(2)(iii)) in addition to ONC's direct investigation of certified health IT for potential safety risks (*see* § 170.580(a)(2)(i)).

6. Concurrent Enforcement by the Office of Inspector General

We clarify that the enforcement approach described in this proposal would apply to ONC's administration of the Conditions and Maintenance of Certification and other requirements under the Program but would not apply to other agencies or offices that have independent authority to investigate and take enforcement action against a health IT developer of certified health IT. Notably, section 3022(b)(1)(A)(ii) of the PHSA, as added by the Cures Act, authorizes the OIG to investigate claims that a health IT developer of certified health IT has engaged in information blocking, which is defined by section 3022(a)(1) of the PHSA subject to reasonable and necessary activities identified by the Secretary as exceptions to the definition as proposed at part 171 (see section VIII. of this proposed rule). Additionally, section 3022(b)(1)(A)(i) authorizes OIG to investigate claims that a health IT developer of certified health IT has submitted a false attestation under the Condition of Certification described at section 3001(c)(5)(D)(vii). We emphasize that ONC's and OIG's respective authorities under the Cures Act (and in general) are independent and that either or both offices may exercise those authorities at any time.

We anticipate, however, that ONC and OIG may coordinate their respective enforcement activities, as appropriate, such as by sharing information about claims or suggestions of possible information blocking or false attestations (including violations of Conditions and Maintenance of Certification that may indicate that a developer has falsely attested to meeting a condition). Therefore, we propose that we may coordinate our review of a claim of information blocking with the OIG or defer to the OIG to lead a review of a claim of information blocking. In addition, we propose that we may rely on OIG findings to form the basis of a direct review action.

7. Applicability of Conditions and Maintenance of Certification Requirements for Self-Developers

The final rule establishing ONC's Permanent Certification Program, "Establishment of the Permanent Certification for Health Information" (76 FR 1261), addresses self-developers. The language in the final rule describes the concept of "self-developed" as referring to a Complete EHR or EHR Module designed, created, or modified by an entity that assumed the total costs for testing and certification and that will be the primary user of the health IT (76 FR 1300). Therefore, self-developers differ from other health IT developers in that their products are not made commercially available and they do not have customers. While we propose that all general Conditions and Maintenance of Certification requirements apply to such developers, we also seek comment on which *aspects* of the Conditions and Maintenance of Certification requirements may not be applicable to self-developers. For example, when considering the Communications Condition of Certification, a self-developer of health IT may not have customer contracts, but could have other agreements in place, such as NDAs, that would be subject to the Condition of Certification.

VIII. Information Blocking

A. Statutory Basis

Section 4004 of the Cures Act added section 3022 of the PHSA (42 U.S.C. 300jj–52, ''the information blocking provision''). Section 3022(a)(1) of the PHSA defines practices that constitute information blocking when engaged in by a health care provider, or a health information technology developer, exchange, or network. Section 3022(a)(3) authorizes the Secretary to identify, through notice and comment rulemaking, reasonable and necessary activities that do not constitute information blocking for purposes of the definition set forth in section 3022(a)(1). We propose to establish seven exceptions to the information blocking definition, each of which would define certain activities that would not constitute information blocking for purposes of section 3022(a)(1) of the PHSA because they are reasonable and necessary to further the ultimate policy goals of the information blocking provision. We also propose to interpret or define certain statutory terms and concepts that are ambiguous, incomplete, or provide the Secretary with discretion, and that we believe are necessary to carry out the Secretary's rulemaking responsibilities under section 3022(a)(3).

B. Legislative Background and Policy Considerations

In this section, we outline the purpose of the information blocking provision and related policy and practical considerations that we considered in identifying the reasonable and necessary activities that are proposed as exceptions to the definition of information blocking described subsequently in section VIII.D of this preamble.

1. Purpose of the Information Blocking Provision

The information blocking provision was enacted in response to concerns that some individuals and entities are engaging in practices that unreasonably limit the availability and use of electronic health information (EHI) for authorized and permitted purposes. These practices undermine public and private sector investments in the nation's health IT infrastructure and frustrate efforts to use modern technologies to improve health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care consumers.

The nature and extent of information blocking has come into sharp focus in recent years. In 2015, at the request of Congress, we submitted a Report on Health Information Blocking[101] (''Information Blocking Congressional Report''), in which we commented on the then current state of technology and of health IT and health care markets. Notably, we observed that prevailing market conditions create incentives for some individuals and entities to exercise their control over EHI in ways that limit its availability and use.

Since that time, we have continued to receive complaints and reports of information blocking from patients, clinicians, health care executives, payers, app developers and other technology companies, registries and health information exchanges, professional and trade associations, and many other stakeholders. ONC has listened to and reviewed these complaints and reports, consulted with stakeholders, and solicited input from our federal partners in order to inform our proposed information blocking policies. Stakeholders described discriminatory pricing policies that have the obvious purpose and effect of excluding competitors from the use of interoperability elements. Many of the industry stakeholders who shared their perspectives with us in listening sessions, including several health IT developers of certified health IT, condemned these practices and urged us to swiftly address them. Our engagement with stakeholders confirms that, despite significant public and private sector efforts to improve interoperability and data accessibility, adverse incentives remain and continue to undermine progress toward a more connected health system.

Based on these economic realities and our first-hand experience working with the health IT industry and stakeholders, in the Information Blocking Congressional Report, we concluded that information blocking is a serious problem and recommended that Congress prohibit information blocking and provide penalties and enforcement mechanisms to deter these harmful practices.

Recent empirical and economic research further underscores the intractability of this problem and its harmful effects. In a national survey of health information organizations, half of respondents reported that EHR developers routinely engage in information blocking, and a quarter of respondents reported that hospitals and health systems routinely do so. The survey reported that perceived motivations for such conduct included, for EHR vendors, maximizing short-term revenue and competing for new clients, and for hospitals and health systems, strengthening their competitive position relative to other hospitals and health systems.[102] Other research suggests that these practices weaken competition among health care providers by limiting patient mobility, encouraging consolidation, and creating barriers to entry for developers of new and innovative applications and technologies that enable more effective uses of clinical data to improve population health and the patient experience.[103]

The information blocking provision provides a comprehensive response to these concerns. The information blocking provision defines and creates possible penalties and disincentives for

[101] ONC, Report to Congress on Health Information Blocking (Apr. 2015), *https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf* [hereinafter ''Information Blocking Congressional Report''].

[102] *See, e.g.,* Julia Adler-Milstein and Eric Pfeifer, *Information Blocking: Is It Occurring And What Policy Strategies Can Address It?,* 95 Milbank Quarterly 117, 124–25 (Mar. 2017), *available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full.*

[103] *See, e.g.,* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, *Making Health Care Markets Work: Competition Policy for Health Care,* 16–17 (Apr. 2017), *available at http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930;* Diego A. Martinez et al., *A Strategic Gaming Model For Health Information Exchange Markets,* Health Care Mgmt. Science (Sept. 2016). (''[S]ome healthcare provider entities may be interfering with HIE across disparate and unaffiliated providers to gain market advantage.'') Niam Yaraghi, *A Sustainable Business Model for Health Information Exchange Platforms: The Solution to Interoperability in Healthcare IT* (2015), *available at http://www.brookings.edu/research/papers/2015/01/30-sustainable-business-model-health-information-exchange-yaraghi;* Thomas C. Tsai & Ashish K. Jha, *Hospital Consolidation, Competition, and Quality: Is Bigger Necessarily Better?,* 312 J. AM. MED. ASSOC. 29, 29 (2014).

information blocking in broad terms, while working to deter the entire spectrum of practices that unnecessarily impede the flow of EHI or its use to improve health and the delivery of care. The information blocking provision applies to the conduct of health care providers, and to health IT developers of certified health IT, exchanges, and networks, and seeks to deter it with substantial penalties, including civil money penalties, and disincentives for violations. Additionally, developers of health IT certified under the Program are prohibited from information blocking under 3001(c)(5)(D)(i) of the PHSA. To promote effective enforcement, the information blocking provision empowers the HHS Office of Inspector General (OIG) to investigate claims of information blocking and provides referral processes to facilitate coordination with other relevant agencies, including ONC, the HHS Office for Civil Rights (OCR), and the Federal Trade Commission (FTC). The information blocking provision also provides for a complaint process and corresponding confidentiality protections to encourage and facilitate the reporting of information blocking. Enforcement of the information blocking provision is buttressed by section 3001(c)(5)(D)(i) and (vi) of the PHSA, which prohibits information blocking by developers of certified health IT as a Condition and Maintenance of Certification requirement under the Program and requires them to attest that they have not engaged in such practices.

2. Policy Considerations and Approach to the Information Blocking Provision

To ensure that individuals and entities that engage in information blocking are held accountable, the information blocking provision encompasses a relatively broad range of potential practices. For example, it is possible that some activities that are innocuous, or even beneficial, could technically implicate the information blocking provision. Given the possibility of these practices, Congress authorized the Secretary to identify reasonable and necessary activities that do not constitute information blocking (see section 3022(a)(3) of the PHSA) (in this proposed rule, we refer to such reasonable and necessary activities identified by the Secretary as ‘‘exceptions’’ to the information blocking provision). The information blocking provision also excludes from the definition of information blocking practices that are required by law (section 3022(a)(1) of the PHSA) and clarifies certain other practices that would not be penalized (sections 3022(a)(6) and (7) of the PHSA).

In considering potential exceptions to the information blocking provision, we must balance a number of policy and practical considerations. To minimize compliance and other burdens for stakeholders, we seek to promote policies that are clear, predictable, and administrable. In addition, we seek to implement the information blocking provision in a way that is sensitive to legitimate practical challenges that may prevent access, exchange, or use of EHI in certain situations. We must also accommodate practices that, while they may inhibit access, exchange, or use of EHI, are reasonable and necessary to advance other compelling policy interests, such as preventing harm to patients and others, promoting the privacy and security of EHI, and promoting competition and consumer welfare.

At the same time, while pursuing these objectives, we must adhere to Congress's plainly expressed intent to provide a comprehensive response to the information blocking problem. Information blocking can occur through a variety of business, technical, and organizational practices that can be difficult to detect and that are constantly changing as technology and industry conditions evolve. The statute responds to these challenges by defining information blocking broadly and in a manner that allows for careful consideration of relevant facts and circumstances in individual cases.

Accordingly, we propose to establish certain defined exceptions to the information blocking provision. These exceptions would be subject to strict conditions that balance the considerations described above. Based on those considerations, in developing the proposed exceptions, we applied three overarching policy criteria. First, each exception would be limited to certain activities that are both reasonable and necessary to advance the aims of the information blocking provision. These reasonable and necessary activities include: Promoting public confidence in the health IT infrastructure by supporting the privacy and security of EHI, and protecting patient safety; and promoting competition and innovation in health IT and its use to provide health care services to consumers. Second, we believe that each exception addresses a significant risk that regulated individuals and entities will not engage in these reasonable and necessary activities because of uncertainty regarding the breadth or applicability of the information blocking provision. Third, and last, each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to protect and does not extend protection to other activities or practices that could raise information blocking concerns.

We discuss these policy considerations in more detail in the context of each of the exceptions proposed in section VIII.D of this preamble.

C. Relevant Statutory Terms and Provisions

In this section of the preamble, we discuss how we propose to interpret certain aspects of the information blocking provision that we believe are ambiguous, incomplete, or that provide the Secretary with discretion. We propose to define or interpret certain terms or concepts that are present in the statute and, in a few instances, to establish new regulatory terms or definitions that we believe are necessary to implement the Secretary's authority under section 3022(a)(3) to identify reasonable and necessary activities that do not constitute information blocking. Our goal in interpreting the statute and defining relevant terms is to provide greater clarity concerning the types of practices that could implicate the information blocking provision and, relatedly, to more effectively communicate the applicability and scope of the proposed exceptions outlined in this proposed rule. We believe that these proposals will provide a more meaningful opportunity for the public to comment on the proposed exceptions and our overall approach to interpreting and administering the information blocking provision. Additionally, we believe additional interpretive clarity will assist regulated actors to comply with the requirements of the information blocking provision.

1. ‘‘Required by Law’’

With regard to the statute's exclusion of practices that are ‘‘required by law’’ from the definition of information blocking, we emphasize that ‘‘required by law’’ refers specifically to interferences with access, exchange, or use of EHI that are explicitly required by state or federal law. By carving out practices that are ‘‘required by law,’’ the statute acknowledged that there are state and federal laws that advance important policy interests and objectives by restricting access, exchange, and use of their EHI, and that practices that follow such laws should not be considered information blocking.

We note that for the purpose of developing an exception for reasonable and necessary privacy-protective practices, we have distinguished between interferences that are ''required by law'' and those engaged in pursuant to a privacy law, but which are not ''required by law.'' The former does not fall within the definition of information blocking, but the latter may implicate the information blocking provision and an exception may be necessary. For a detailed discussion of this topic, please see section VIII.D.2 of this preamble.

2. Health Care Providers, Health IT Developers, Exchanges, and Networks

Section 3022(a)(1) of the PHSA, in defining information blocking, refers to four classes of individuals and entities that may engage in information blocking and which include: Health care providers, health IT developers of certified health IT, networks, and exchanges. We propose to adopt definitions of these terms to provide clarity regarding the types of individuals and entities to whom the information blocking provision applies. We note that, for convenience and to avoid repetition in this preamble, we typically refer to these individuals and entities covered by the information blocking provision as ''actors'' unless it is relevant or useful to refer to the specific type of individual or entity. That is, when the term ''actor'' appears in this preamble, it means an individual or entity that is a health care provider, health IT developer, exchange, or network. For the same reasons, we propose to define ''actor'' in § 171.102.

a. Health Care Providers

The term ''health care provider'' is defined in section 3000(3) of the PHSA. We propose to adopt this definition for purposes of section 3022 of the PHSA when defining ''health care provider'' in § 171.102. We note that this definition is different from the definition of ''health care provider'' under the HIPAA Privacy and Security Rules. We are considering adjusting the information blocking definition of ''health care provider'' to cover all individuals and entities covered by the HIPAA ''health care provider'' definition. We seek comment on whether this approach would be justified, and commenters are encouraged to specify reasons why doing so might be necessary to ensure that the information blocking provision applies to all health care providers that might engage in information blocking.

b. Health IT Developers of Certified Health IT

Section 3022(a)(1)(B) of the PHSA defines information blocking, in part, by reference to the conduct of ''health information technology developers.'' Because title XXX of the PHSA does not define ''health information technology developer,'' we interpret section 3022(a)(1)(B) in light of the specific authority provided to OIG in section 3022(b)(1)(A) and (b)(2). Section 3022(b)(2) discusses developers, networks, and exchanges in terms of an ''individual or entity,'' specifically cross-referencing section 3022(b)(1)(A). Sections 3002(b)(1) and (b)(1)(A) state, in relevant part, that the OIG may investigate information blocking claims regarding a health information technology developer of certified health information technology or other entity offering certified health information technology. Together, these sections make clear that the information blocking provisions and OIG's authority extend to individuals *or* entities that develop *or* offer certified health IT. That the individual or entity must develop or offer *certified* health IT is further supported by section 3022(a)(7) of the PHSA—which refers to developers' responsibilities to meet the requirements of certification—and section 4002 of the Cures Act—which identifies information blocking as a Condition of Certification.

Notwithstanding this, the Cures Act does not prescribe that conduct that may implicate the information blocking provisions be limited to practices related to *only* certified health IT. Rather, the information blocking provisions would be implicated by any practice engaged in by an individual or entity that develops or offers certified health IT that is likely to interfere with the access, exchange, or use of EHI, including practices associated with *any* of the developer or offeror's health IT products that have *not* been certified under the Program. This interpretation is based primarily on section 3022(b)(1) of the PHSA. If Congress had intended that the enforcement of the information blocking provisions were limited to practices connected to certified health IT, we believe the Cures Act would have included language that tied enforcement to the operation or performance of a product certified under the Program. Rather, the description of the practices that OIG can investigate in section 3022(b)(1)(A)(ii) of the PHSA are not tied to the certification status of the health IT at issue, omitting any express reference to a health IT developer's practice needing to be related to ''certified health information technology.'' That the scope of the information blocking provision should not be limited to practices that involve only certified health IT is further evidenced by no such limitation applying to health care providers, health information exchanges (HIEs), and health information networks (HINs) as listed in sections 3022(b)(1) of the PHSA.

Additionally, the ''practice described'' in section 3022(a)(2) of the PHSA refers to ''certified health information technologies'' when illustrating practices that restrict authorized access, exchange, or use of EHI under applicable state or federal laws (section 3022(a)(2)(A) of the PHSA), but omits any reference to certification when describing ''health information technology'' in the practices described in sections 3022(a)(2)(B) and (C) of the PHSA. Importantly, sections 3022(a)(2)(B) and (C) of the PHSA address practices that are particularly relevant to health IT developers and offerors, although they could be engaged in by other types of actors. We interpret this drafting as a deliberate decision not to link the information blocking provisions with only the performance or use of certified health IT.

Finally, we note that the Cures Act does not impose a temporal nexus that would require that information blocking be carried out at a time when an individual or entity had health IT certified under the Program. Ostensibly, then, once an individual or entity has health IT certified, or otherwise maintains the certification of health IT, the individual or entity becomes forever subject to the information blocking provision. We do not believe that, understood in context, the Cures Act supports such a broad interpretation. Noting the above discussion concerning OIG's scope of authority under section 3022(b)(1)(A) and (b)(2) of the PHSA, we believe that to make developers and offerors of certified health IT subject to the information blocking provision in perpetuity would be inconsistent with the voluntary nature of the Program. However, we also believe that the Cures Act does not provide any basis for interpreting the information blocking provision so narrowly that a developer or offeror of certified health IT could escape penalty as a consequence of having its certification terminated or by withdrawing all of its extant certifications.

We consider that in the circumstances where a health IT developer has its certification terminated, or withdraws its certification, such that it no longer has any health IT certified under the

Program, it should nonetheless be subject to penalties for information blocking engaged in during the time that it did have health IT certified under the Program. Accordingly, we propose to adopt a definition of ''heath information technology (IT) developer of certified health IT'' for the purposes of interpretation and enforcement of the information blocking provisions, including those regulatory provisions proposed under Title 45, part 171, of the Code of Federal Regulations, that would capture such developers or offerors. We propose, in § 171.102, that ''health IT developer of certified health IT'' means an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health IT (one or more) certified under the Program. To note, we propose that the term ''information blocking claim'' within this definition should be read broadly to encompass any statement of information blocking or potential information blocking. ''Claims'' of information blocking within this definition would not be limited, in any way, to a specific form, format, or submission approach or process.

We are also considering additional approaches to help ensure that developers and offerors of certified health IT remain subject to the information blocking provision for an appropriate period of time after leaving the Program. The rationale for this approach would be that a developer or offeror of certified health IT should be subject to penalties if, following the termination or withdrawal of certification, it refused to provide its customers with access to the EHI stored in the decertified health IT, provided that such interference was not required by law and did not qualify for one of the information blocking exceptions. Adopting this broader approach would help avoid the risk that a developer would be able to engage in the practices described in section 3022(a)(2) of the PHSA in respect to EHI that was collected on behalf of a health care provider when that health care provider would reasonably expect that the information blocking provision would protect against unreasonable and unnecessary interferences with that EHI. If the information blocking provision did not extend to capture such conduct, the protection afforded by the information blocking provision could become illusory, and providers would need to consider securing contractual rights to prevent interference, which we are aware they typically have great difficulty doing.[104]

One way that this could be achieved would be to define ''health IT developer of certified health IT'' as including developers and offerors of certified health IT that continue to store EHI that was previously stored in health IT certified in the Program. Alternatively, we are considering whether developers and offerors of certified health IT should remain subject to the information blocking provision for an appropriate period of time after leaving the Program. Namely, that the information blocking provision should apply for a specific time period, say one year, after the developer or offeror no longer has any health IT certified in the Program. This second approach has the attraction of providing a more certain basis for understanding which developers are subject to the information blocking provision. However, it also potentially captures developers and offerors who have fully removed themselves from the Program and, for example, no longer exercise control over EHI that was stored in their certified health IT.

We seek comment on which of these two models best achieves our policy goal of ensuring that health IT developers of certified health IT will face consequences under the information blocking provision if they engage in information blocking in connection with EHI that was stored or controlled by the developer or offeror whilst they were participating in the program. Commenters are also encouraged to identify alternative models and approaches for identifying when a developer or offeror should, and should no longer, be subject to the information blocking provision.

We note that a developer or offeror of a single health IT product that has had its certification suspended would be considered to *have* certified health IT for the purpose of the definition. We also note that we interpret the requirement that the health IT developer of certified health IT ''exercise control'' over EHI broadly. A developer would not necessarily need to have access to the EHI in order to exercise control. For example, a developer that implemented a ''kill-switch'' for a decertified software product that was locally hosted by a health care provider, preventing that provider from accessing its records, would be exercising control over the EHI for the purpose of this definition.

We clarify that we interpret ''individual or entity that develops the certified health IT'' as the individual or entity that is legally responsible for the certification status of the health IT, which would be the individual or entity that entered into a binding agreement that resulted in the certification status of the health IT under the Program or, if such rights are transferred, the individual or entity that holds the rights to the certified health IT. We also clarify that an ''individual or entity that offers certified health IT'' would include an individual or entity that under any arrangement makes certified health IT available for purchase or license. We seek comment on both of our interpretations. More specifically, we seek comment on whether there are particular types of arrangements under which certified health IT is ''offered'' in which the offeror should not be considered a ''health IT developer of certified health IT'' for the purposes of the information blocking provisions.

We also clarify that the proposed definition of ''health IT developer of certified health IT'' and our interpretation of the use of ''health information technology developer'' applies to Part 171 only and does not apply to the implementation of any other section of the PHSA or the Cures Act, including section 4005(c)(1) of the Cures Act.

We clarify that API Technology Suppliers, as described in section VII.4 of this preamble and defined in § 170.102, would be considered health IT developers of certified health IT subject to the conditions described above.

Last, we clarify that a ''self-developer'' of certified health IT, as the term has been used in the ONC Health IT Certification Program (Program) and described in this rulemaking (section VII.D.7) and previous rulemaking,[105] would be treated as a health care provider for the purposes of information blocking. This is because of our description of a self-developer for Program purposes[106] would essentially mean that such developers would not be supplying or offering their certified health IT to other entities. To be clear, self-developers would still be subject to the proposed Conditions and

[104] *See* ONC, *EHR Contracts Untangled Selecting Wisely, Negotiating Terms, And Understanding The Fine Print, https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf* (September 2016).

[105] The final rule establishing ONC's Permanent Certification Program, ''Establishment of the Permanent Certification for Health Information'' (76 FR 1261), addresses self-developers.

[106] The language in the final rule describes the concept of ''self-developed'' as referring to a complete EHR or EHR Module designed, created, or modified by an entity that assumed the total costs for testing and certification and that will be the primary user of the health IT (76 FR 1300).

Maintenance of Certification requirements because they have health IT certified under the Program (*see also* section VII.D.7). We welcome comments on our determination regarding ''self-developers'' for information blocking purposes and whether there are other factors we should consider in how we treat ''self-developers'' of certified health IT for the purposes of information blocking.

We also seek comment generally on the definition proposed for ''health IT developer of certified health IT.''

c. Networks and Exchanges

The terms ''network'' and ''exchange'' are not defined in the information blocking provision or in any other relevant statutory provisions. We propose to define these terms so that these individuals and entities that are covered by the information blocking provision understand that they must comply with its provisions. In accordance with the meaning and intent of the information blocking provision, we believe it is necessary to define these terms in a way that does not assume the application or use of certain technologies and is flexible enough to apply to the full range and diversity of exchanges and networks that exist today and may arise in the future. We note that in the past few years alone many new types of exchanges and networks that transmit EHI have emerged, and we expect this trend to accelerate with continued advancements in technology and renewed efforts to advance trusted exchange among networks and other entities under the trusted exchange framework and common agreement provided for by section 4003(b) of the Cures Act.

In considering the most appropriate way to define these terms, we examined how they are used throughout the Cures Act and the HITECH Act. Additionally, we considered dictionary and industry definitions of ''network'' and ''exchange.'' While these terms have varied usage and meaning in different industry contexts, certain concepts are common and have been incorporated into the proposed definitions below.

i. Health Information Network

We propose a functional definition of ''health information network'' (HIN) that focuses on the role of these actors in the health information ecosystem. We believe the defining attribute of a HIN is that it enables, facilitates, or controls the movement of information between or among different individuals or entities that are unaffiliated. For this purpose, we propose that two parties are affiliated if one has the power to control the other, or if both parties are under the common control or ownership of a common owner. We note that a significant implication of this definition is that a health care provider or other entity that enables, facilitates, or controls the movement of EHI within its own organization, or between or among its affiliated entities, is not a HIN in connection with that movement of information for the purposes of this proposed rule.

More affirmatively, we propose that an actor could be considered a HIN if it performs any or any combination of the following activities. First, the actor would be a HIN if it were to determine, oversee, administer, control, or substantially influence policies or agreements that define the business, operational, technical, or other conditions or requirements that enable or facilitate the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities. Second, an actor would be a HIN if it were to provide, manage, control, or substantially influence any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.

Typically, a HIN will influence the sharing of EHI between many unaffiliated individuals or entities. However, we do not propose to establish any minimum number of parties or ''nodes'' beyond the requirement that there be some actual or contemplated access, exchange, or use of information between or among at least two unaffiliated individuals or entities that is enabled, facilitated, or controlled by the HIN. We believe such a limitation would be artificial and would not capture the full range of entities that should be considered networks under the information blocking provision. To be clear, any individual or entity that enables, facilitates, or controls the access, exchange, or use of EHI between or among only itself and another unaffiliated individual or entity would not be considered a HIN in connection with the movement of that EHI (although that movement of EHI may still be regulated under the information blocking provision on the basis that the individual or entity is a health care provider or health IT developer of certified health IT). To be a HIN, the individual or entity would need to be enabling, facilitating, or controlling the access, exchange, or use of EHI between or among two or more *other* individuals or entities that were not affiliated with it.

To illustrate how the proposed definition would operate, we note the following examples. An entity is established within a state for the purpose of improving the movement of EHI between the health care providers operating in that state. The entity identifies standards relating to security and offers terms and conditions to be entered into by health care providers wishing to participate in the network. The entity offering (and then overseeing and administering) the terms and conditions for participation in the network would be considered a HIN for the purpose of the information blocking provision. We note that there is no need for a separate entity to be created in order that an entity be considered a HIN. For instance, a health system that administers business and operational agreements for facilitating the exchange of EHI that are adhered to by unaffiliated family practices and specialist clinicians in order to streamline referrals between those practices and specialists would likely be considered a HIN.

We note that the proposed definition would also encompass an individual or entity that does not directly enable, facilitate, or control the movement of information, but nonetheless exercises control or substantial influence over the policies, technology, or services of a network. In particular, there may be an individual or entity that relies on another entity—such as an entity specifically created for the purpose of managing a network—for policies and technology, but nevertheless dictates the movement of EHI over that network. For example, a large health care provider may decide to lead an effort to establish a network that facilitates the movement of EHI between a group of smaller health care providers (as well as the large health care provider) and through the technology of health IT developers. To achieve this outcome, the large health care provider, together with some of the participants, creates a new entity that administers the network's policies and technology. In this scenario, the large health care provider would come within the functional definition of a HIN and could be held accountable for the conduct of the network if the large health care provider used its control or substantial influence over the new entity—either in a legal sense, such as via its control over the governance or management of the entity, or in a less formal sense, such as if the large health care provider prescribed a policy to be adopted—to interfere with the access, exchange, or use of EHI. We note that the large health care provider in this example would be treated as a health care provider when utilizing the network to move EHI via the network's policies, technology, or services, but would be considered a HIN in connection with the practices of the network over which the large health care provider exercises control or substantial influence.

We seek comment on the proposed definition of a HIN. In particular, we request comment on whether the proposed definition is broad enough (or too broad) to cover the full range of individuals and entities that could be considered health information networks within the meaning of the information blocking provision. Additionally, we specifically request comment on whether the proposed definition would effectuate our policy goal of defining this term in a way that does not assume particular technologies or arrangements and is flexible enough to accommodate changes in these and other conditions.

ii. Health Information Exchange

We propose to define a ''health information exchange'' (HIE) as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. Our research and experience in working with exchanges drove the proposed definition of this term. HIEs include but are not limited to regional health information organizations (RHIOs), state health information exchanges (state HIEs), and other types of organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used between or among particular types of parties or for particular purposes. For example, an HIE might facilitate or enable the access, exchange, or use of EHI exclusively within a regional area (such as a RHIO), or for a limited scope of participants and purposes (such as a clinical data registry or an exchange established by a hospital-physician organization to facilitate Admission, Discharge, and Transfer (ADT) alerting). We note that HIEs may be established under federal or state laws or regulations but may also be established for specific health care or business purposes or use cases. Additionally, we note that if an HIE facilitates the access, exchange, or use of EHI for more than a narrowly defined set of purposes, then it may be both an HIE and a HIN.

We seek comment on this proposed definition of an HIE. Again, we encourage commenters to consider whether this proposed definition is broad enough (or too broad) to cover the full range of individuals and entities that could be considered exchanges within the meaning of the information blocking provision, and whether the proposed definition is sufficiently flexible to accommodate changing technological and other conditions.

3. Electronic Health Information

The definition of information blocking applies to *electronic* health information (EHI) (section 3022(a)(1) of the PHSA). While section 3000(4) of the PHSA by reference to section 1171(4) of the Social Security Act defines ''health information,'' EHI is not specifically defined in the Cures Act, HITECH Act, or other relevant statutes. We propose to define EHI to mean:

(i) Electronic protected health information; and

(ii) any other information that—

- is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103;
- identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
- relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

This definition of EHI includes, but is not limited to, electronic protected health information and health information that is created or received by a health care provider and those operating on their behalf; health plan; health care clearinghouse; public health authority; employer; life insurer; school; or university. In addition, we clarify that under our proposed definition, EHI includes, but is not limited to, electronic protected health information (ePHI) as defined in 45 CFR 160.103. In particular, unlike ePHI and health information, EHI is not limited to information that is created or received by a health care provider, health plan, health care clearinghouse, public health authority, employer, life insurer, school, or university. EHI may be provided, directly from an individual, or from technology that the individual has elected to use, to an actor covered by the information blocking provisions. We propose that EHI does not include health information that is de-identified consistent with the requirements of 45 CFR 164.514(b). We generally request comment on this proposed definition as well as on whether the exclusion of health information that is de-identified is consistent with the requirements of 45 CFR 164.514(b).

To be clear, this definition provides for an expansive set of EHI, which could include information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information.

Price Information

The fragmented and complex nature of pricing within the health care system has decreased the efficiency of the health care system and has had negative impacts on patients, health care providers, health systems, plans, plan sponsors and other key health care stakeholders. Patients and plan sponsors have trouble anticipating or planning for costs, are not sure how they can lower their costs, are not able to compare costs, and have no practical way to measure the quality of the care or coverage they receive relative to the price they pay. Pricing information continues to grow in importance with the increase of high deductible health plans and surprise billing, which have resulted in an increase in out-of-pocket health care spending. Transparency in the price and cost of health care would help address the concerns outlined above by empowering patients to make informed health care decisions. Further, the availability of price information could help increase competition that is based on the quality and value of the services patients receive. Consistent with its statutory authority, the Department is considering subsequent rulemaking to expand access to price information for the public, prospective patients, plan sponsors, and health care providers.

Increased consumer demand, aligned incentives, more accessible and digestible information, and the evolution of price transparency tools are critical components to moving to a health care system that pays for value. However, the complex and decentralized nature of how price information is created, structured, formatted, and stored presents many challenges to achieving price transparency. To this point, pricing within health care demands a market-based approach whereby, for example, platforms are created that utilize raw data to provide consumers with digestible price information through their preferred medium.

ONC has a unique role in setting the stage for such future actions by establishing the framework to prevent the blocking of price information. Given that price information impacts the ability of patients to shop for and make decisions about their care, we seek comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking. In addition, the overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

- Should prices that are included in EHI:
  - ○ Reflect the amount to be charged to and paid for by the patient's health plan (if the patient is insured) and the amount to be charged to and collected from the patient (as permitted by the provider's agreement with the patient's health plan), including for drugs or medical devices;
  - ○ Include various pricing information such as charge master price, negotiated prices, pricing based on CPT codes or DRGs, bundled prices, and price to payer;
  - ○ Be reasonably available in advance and at the point of sale;
  - ○ Reflect all out-of-pocket costs such as deductibles, copayments and coinsurance (for insured patients); and/or
  - ○ Include a reference price as a comparison tool such as the Medicare rate and, if so, what is the most meaningful reference?
- For the purpose of informing referrals for additional care and prescriptions, should future rulemaking by the Department require health IT developers to include in their platforms a mechanism for patients to see price information, and for health care providers to have access to price information, tailored to an individual patient, integrated into the practice or clinical workflow through APIs?
- To the extent that patients have a right to price information within a reasonable time in advance of care, how would such reasonableness be defined for:
  - ○ Scheduled care, including how far in advance should such pricing be available for patients still shopping for care, in addition to those who have already scheduled care;
  - ○ Emergency care, including how and when transparent prices should be disclosed to patients and what sort of exceptions might be appropriate, such as for patients in need of immediate stabilization;
  - ○ Ambulance services, including air ambulance services; and
  - ○ Unscheduled inpatient care, such as admissions subsequent to an emergency visit?
- How would price information vary based on the type of health insurance and/or payment structure being utilized, and what, if any, challenges would such variation create to identifying the price information that should be made available for access, exchange, or use?
- Are there electronic mechanisms/processes available for providing price information to patients who are not registered (*i.e.,* not in the provider system) when they try to get price information?
- Should price information be made available on public websites so that patients can shop for care without having to contact individual providers, and if so, who should be responsible for posting such information? Additionally, how would the public posting of pricing information through API technology help advance market competition and the ability of patients to shop for care?
- If price information that includes a provider's negotiated rates for all plans and the rates for the uninsured were to be required to be posted on a public website, is there technology currently available or that could be easily developed to translate that data into a useful format for individuals? Are there existing standards and code sets that would facilitate such transmission and translation? To the extent that some data standards are lacking in this regard, could developers make use of unstandardized data?
- What technical standards currently exist or may be needed to represent price information electronically for purposes of access, exchange, and use?
- Are there technical impediments experienced by stakeholders regarding price information flowing electronically?
- Would updates to the CMS-managed HIPAA transactions standards and code sets be necessary to address the movement of price information in a standardized way?
- How can price transparency be achieved for care delivered through value based arrangements, including at accountable care organizations, demonstrations and other risk-sharing arrangements?
- What future requirements should the Department consider regarding the inclusion of price information in a patient's EHI, particularly as it relates to the amount paid to a health care provider by a patient (or on behalf of a patient) as well as payment calculations for the future provision of health care to such patient?
- If price information is included in EHI, could that information be useful in subsequent rulemaking that the Department may consider in order to reduce or prevent surprise medical billing, such as requirements relating to:
  - ○ The provision of a single bill that includes all health care providers involved in a health care service, including their network status;
  - ○ The provision of a binding quote reasonably in advance of scheduled care (that is, non-emergent care) or some subset of scheduled care, such as for the most ''shoppable'' services;
  - ○ Ensuring that all health care providers in an in-network facility charge the in-network rate; and
  - ○ Notification of billing policies such as timely invoice dates for all providers and facilities, notwithstanding network status, due date for invoice payments by the prospective patient's payers and out-of-pocket obligations, date when unpaid balances are referred for collections, and appeals rights and procedures for patients wishing to contest an invoice?

4. Interests Promoted by the Information Blocking Provision

a. Access, Exchange, and Use of EHI

The information blocking provision promotes the ability to *access, exchange, and use* EHI, consistent with the requirements of applicable law. We interpret the terms ''access,'' ''exchange,'' and ''use'' broadly, consistent with their generally understood meaning in the health IT industry and their function and context in the information blocking provision.

The concepts of access, exchange, and use are closely related: EHI cannot be used unless it can be accessed, and this often requires that the EHI be exchanged among different individuals or entities and through various technological means. Moreover, the technological and other means necessary to facilitate appropriate access and exchange of EHI vary significantly depending on the purpose for which the information will be used. For example, the technologies and services that support a payer's access to EHI to assess clinical value will likely differ from those that support a patient's access to EHI via a smartphone app. That is, to deter information blocking in these and many other potential uses of EHI—and, by extension, the many and diverse means of access and exchange that support such uses.

This is consistent with the way these terms are employed in the information blocking provision and in other relevant statutory provisions. For example, section 3022(a)(2) of the PHSA contemplates a broad range of purposes for which EHI may be accessed, exchanged, and used—from treatment, care delivery, and other permitted purposes, to exporting complete information sets and transitioning between health IT systems, to supporting innovations and advancements in health information access, exchange, and use. Separately, the Cures Act and the HITECH Act contemplate many different purposes for and means of accessing, exchanging, and using EHI, which include, but are not limited to, quality improvement, guiding medical decisions at the time and place of care, reducing medical errors and health disparities, delivering patient-centered care, and supporting public health and clinical research activities.[107]

In addition to these statutory provisions, we have considered how the terms access, exchange, and use have been defined or used in existing regulations and other relevant health IT industry contexts. While those definitions have specialized meanings and are not controlling here, they are instructive insofar as they illustrate the breadth with which these terms have been understood in other contexts. For example, the HIPAA Privacy Rule defines an individual's right of access to include the right to have a copy of all or part of their PHI transmitted directly to them or any person or entity he or she designates, in any form and format (including electronically) that the individual requests and that the covered entity holding the information can readily produce (45 CFR 164.524). In a different context, the HIPAA Security Rule defines ''access'' as the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource (45 CFR 164.304). The HIPAA Rules also define the term ''use,'' which includes the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains the information (45 CFR 160.103).

As the examples and discussion above demonstrate, the concepts of access, exchange, and use are used in a variety of contexts to refer to a broad spectrum of activities. We believe that the types of access, exchange, and use described above would be promoted under the information blocking provision, as would other types of access, exchange, or use not specifically contemplated in these or other regulations. Further, we note that the information blocking provision would also extend to innovations and advancements in health information access, exchange, and use that may occur in the future (see section 3022(a)(2) of the PHSA).

Consistent with the above, and to convey the full breadth of activities that may implicate the information blocking provision, we propose definitions of access, exchange, and use in § 171.102. We emphasize the interrelated nature of the definitions. For example, the definition of ''use'' includes the ability to read, write, modify, manipulate, or apply EHI to accomplish a desired outcome or to achieve a desired purpose, while ''access'' is defined as the ability or means necessary to make EHI available for *use.* As such, interference with ''access'' would include, for example, an interference that prevented a health care provider from writing EHI to its health IT or from modifying EHI stored in health IT, whether by the provider itself or by, or via, a third-party app. We encourage comment on these definitions. In particular, commenters may wish to consider whether these definitions are broad enough to cover all of the potential purposes for which EHI may be needed and ways in which it could conceivably be used, now and in the future.

b. Interoperability Elements

In this proposed rule, we use the term ''interoperability element'' to refer to any means by which EHI can be accessed, exchanged, or used. We clarify that the means of accessing, exchanging, and using EHI are not limited to functional elements and technical information but also encompass technologies, services, policies, and other conditions[108] necessary to support the many potential uses of EHI as described above. Because of the evolving nature of technology and the diversity of privacy laws and regulations, institutional arrangements, and policies that govern the sharing of EHI, we will not provide an exhaustive list of interoperability elements. However, we believe that it is useful to define this term, both because of its importance for analyzing the likelihood of interference under the information blocking provision, and because some of the proposed exceptions to the provision contain conditions concerning the availability and provision of interoperability elements. Therefore, we propose to define ''interoperability element'' in § 171.102. As noted, our intent is to capture all of the potential means by which EHI may be accessed, exchanged, or used for any relevant purposes; both now and as technology and other conditions evolve. We seek comment on whether the proposed definition realizes that intent and, if not, any changes we should consider.

5. Practices That May Implicate the Information Blocking Provision

To meet the definition of information blocking, a practice must be *likely to interfere with, prevent, or materially discourage* access, exchange, or use of EHI. In this section and elsewhere in this preamble, we discuss various types of hypothetical practices that *could* implicate the provision. We do this to illustrate the scope of the information blocking provision and to explain our interpretation of various statutory concepts. However, we stress that the types of practices discussed in this preamble are illustrative, not exhaustive, and that many other types of practices could also implicate the provision. Nor does the fact that we have not identified or discussed a particular type of practice imply that it is less serious than those that are discussed in this preamble. Indeed, because information blocking may take many forms, it is not possible—and we do not attempt—to anticipate or catalog the many potential types of practices that may raise information blocking concerns.

We emphasize that any analysis of information blocking necessarily requires a careful consideration of the individual facts and circumstances, including whether the practice was required by law, whether the actor had the requisite statutory knowledge, and whether an exception applies. When we state that a practice would implicate the provision or *could* violate the provision, we are expressing a conclusion that the type of practice is one that would be likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI, and that further analysis of these and other statutory elements would therefore be warranted to determine whether a violation has occurred. We highlight this distinction because to *implicate* the information blocking provision is *not* necessarily to *violate* it, and that each case will turn on its own unique facts. For example, a practice that seemingly meets the statutory definition of information blocking would not be information blocking if it was required by law, if one or more elements of the definition were not met, or if was covered by one of the proposed exceptions.

We propose in section VIII.D of this preamble to establish seven exceptions to the information blocking provision for certain reasonable and necessary activities. If an actor can establish that an exception applies to each practice for which a claim of information blocking

[107] *See* section 3001(b) of the PHSA; *see also* section 3009(a)(3) of the PHSA (enumerating reporting criteria relating to access, exchange, and use of EHI for a broad and diverse range of purposes).

[108] *See* ONC, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap* at x–xi, *https://www.healthit.gov/topic/interoperability/interoperability-roadmap* (Oct. 2015) [hereinafter ''Interoperability Roadmap''].

has been made, including that the actor satisfied all applicable conditions of the exception at all relevant times, then the practice would not constitute information blocking.

Based on early discussions with stakeholders during the development of this proposed rule, we are aware that the generality with which the information blocking provision describes practices that are likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI may leave some uncertainty as to the scope of the information blocking provision and the types of practices that will implicate enforcement by ONC and/or OIG. To provide additional clarity on this point, we elaborate our understanding of these important statutory concepts below.

a. Prevention, Material Discouragement, and Other Interference

The information blocking provision and its enforcement subsection do not define the terms ''interfere with,'' ''prevent,'' and ''materially discourage,'' and use these terms collectively and without differentiation. Based on our interpretation of the information blocking provision and the ordinary meanings of these terms in the context of EHI, we do not believe they are mutually exclusive, but that prevention and material discouragement are best understood as types of interference, and that use of these terms in the statute to define information blocking illustrates the desire to reach all practices that an actor knows, or should know, are likely to prevent, materially discourage, or otherwise interfere with the access, exchange, or use of EHI. Consistent with this understanding, in this preamble to the proposed rule, we use the terms ''interfere with'' and ''interference'' as inclusive of prevention, material discouragement, and other forms of interference that implicate the information blocking provision.

We believe that interference could take many forms. In addition to the prevention or material discouragement of access, exchange, or use, we propose that interference could include practices that increase the cost, complexity, or other burden associated with accessing, exchanging, or using EHI. Additionally, interference could include practices that limit the utility, efficacy, or value of EHI that is accessed, exchanged, or used, such as by diminishing the integrity, quality, completeness, or timeliness of the data. We refer readers to section VIII.C.5.c of this preamble below for a discussion of these and other potential practices that could interfere with access, exchange, or use and thereby implicate the information blocking provision.

Relatedly, to avoid potential ambiguity and clearly communicate the full range of potential practices that could implicate the information blocking provision, we propose to codify a definition of ''interfere with'' in § 171.102, consistent with our interpretation set forth above.

b. Likelihood of Interference

The information blocking provision is preventative in nature. That is, the information blocking provision proscribes practices that are *likely* to interfere with (including preventing or materially discouraging) access, exchange, or use of EHI—whether or not such harm actually materializes. By including both the likely and the actual effects of a practice, the information blocking provision encourages individuals and entities to avoid engaging in practices that undermine interoperability, and to proactively promote access, exchange, and use of EHI.

We believe that a practice would satisfy the information blocking provision's ''likelihood'' requirement if, under the circumstances, there is a reasonably foreseeable risk that the practice will interfere with access, exchange, or use of EHI. For example, where an actor refuses to share EHI or to provide access to certain interoperability elements, it is reasonably foreseeable that such actions will interfere with access, exchange, or use of EHI. As another example, it is reasonably foreseeable that a health care provider may need to access information recorded in a patient's electronic record that could be relevant to the treatment of that patient. For this reason, a policy or practice that limits timely access to such information in an appropriate electronic format creates a reasonably foreseeable likelihood of interfering with the use of the information for these treatment purposes.

Whether the risk of interference is reasonably foreseeable will depend on the particular facts and circumstances attending the practice or practices at issue. Because of the number and diversity of potential practices, and the fact that different practices will present varying risks of interfering with access, exchange, or use of EHI, we do not attempt to anticipate all of the potential ways in which the information blocking provision could be implicated. Nevertheless, to assist with compliance, we clarify certain circumstances in which, based on our experience, a practice will almost always be likely to interfere with access, exchange, or use of EHI. We caution that these situations are not exhaustive and that other circumstances may also give rise to a very high likelihood of interference under the information blocking provision. In each case, ONC will consider the totality of the circumstances in evaluating whether a practice is likely to implicate the statute and to give rise to a violation.

i. Observational Health Information

Although the information blocking provision applies to all EHI, we believe that information blocking concerns are especially pronounced when the conduct at issue has the potential to interfere with the access, exchange, or use of EHI that is created or maintained during the practice of medicine or the delivery of health care services to patients. We refer to such information in this section of the preamble collectively as ''observational health information.'' Such information includes, but is not limited to, health information about a patient that could be captured in a patient record within an EHR and other clinical information management systems; as well as information maintained in administrative and other IT systems when the information is clinically relevant, directly supports patient care, or facilitates the delivery of health care services to consumers. We note that there is a special need for timely, electronic access to this information and that, moreover, the clinical and operational utility of this information is often highly dependent on multiple actors exercising varying forms and degrees of control over the information itself or the technological, contractual, or other means by which it can be accessed, exchanged, and used. Against these indications, practices that adversely impact the access, exchange, or use of observational health information will almost always implicate the information blocking provision.

We note that observational health information may be technically structured or unstructured (such as ''free text''). Therefore, in general, clinicians' notes would constitute observational health information, at least insofar as the notes contain observations or conclusions about a patient or the patient's care. In contrast, we believe certain types of EHI are qualitatively distinct from observational health information, such as EHI that is created through aggregation, algorithms, and other techniques that transform observational health information into fundamentally new data or insights that are not obvious from the observational information alone. This could include, for example, population-level trends, predictive analytics, risk scores, and EHI used for comparisons and benchmarking activities. Similarly, internally developed quality measures and care protocols are generally distinct from observational health information. In general, we believe that practices that pertain solely to the creation or use of these transformative data and insights would not usually present the very high likelihood of interference described above. However, we emphasize that, depending on the specific facts at issue, practices related to electronic non-observational health information (a type of EHI), such as price information, *could* still be subject to the information blocking provision. We seek comment on this proposed approach and encourage commenters to identify potential practices related to non-observational health information that could raise information blocking concerns.

Finally, we clarify that merely collecting, organizing, formatting, or processing observational health information maintained in EHRs and other source systems does not change the fundamental nature of that EHI or obligations under the information blocking provisions. Likewise, the mere fact that EHI is stored in a proprietary format or has been combined with confidential or proprietary information does not alter the actor's obligations under the information blocking provisions to facilitate access, exchange, and use of the EHI in response to a request. For example, the information blocking provision would be implicated if an actor were to assert proprietary rights in medical vocabularies or code sets in a way that was likely to interfere with the access, exchange, or use of observational health information stored in such formats. However, as noted in section VIII.D.6 of this preamble, under the exception for licensing of interoperability elements on reasonable and non-discriminatory terms, an actor could charge a royalty for access to proprietary data or data coded in a proprietary manner so long as that royalty were offered on reasonable and non-discriminatory terms pursuant to the conditions outlined in the exception.

ii. Purposes for Which Information May be Needed

We believe the information blocking provision will almost always be implicated when a practice interferes with access, exchange, or use of EHI for certain purposes, including but not limited to:

- Providing patients with access to their EHI and the ability to exchange and use it without special effort (*see* section VII.B.4).
- Ensuring that health care professionals, care givers, and other authorized persons have the EHI they need, when and where they need it, to make treatment decisions and effectively coordinate and manage patient care and can use the EHI they may receive from other sources.
- Ensuring that payers and other entities that purchase health care services can obtain the information they need to effectively assess clinical value and promote transparency concerning the quality and costs of health care services.
- Ensuring that health care providers can access, exchange, and use EHI for quality improvement and population health management activities.
- Supporting access, exchange, and use of EHI for patient safety and public health purposes.

The need to ensure that EHI is readily available and usable for these purposes is paramount. Therefore, practices that increase the cost, difficulty, or other burden of accessing, exchanging, or using EHI for these purposes would almost always implicate the information blocking provision. Individuals and entities that develop health IT or have a role in making these technologies and services available should consider the impact of their actions and take steps to support interoperability and avoid impeding the availability or use of EHI.

iii. Control Over Essential Interoperability Elements; Other Circumstances of Reliance or Dependence

An actor may have substantial control over one or more interoperability elements that provide the only reasonable means of accessing, exchanging, or using EHI for a particular purpose. In these circumstances, any practice by the actor that could impede the use of the interoperability elements—or that could unnecessarily increase the cost or other burden of using the elements—would almost always implicate the information blocking provision.

The situation described above is most likely when customers or users are dependent on an actor's technology or services, which can occur for any number of reasons. For example, technological dependence may arise from legal or commercial relations, such as a health care provider's reliance on its EHR developer to ensure that EHI managed on its behalf is accessible and usable when it is needed. Relatedly, most EHI is currently stored in EHRs and other source systems that use proprietary data models or formats. Knowledge of the data models, formats, or other relevant technical information (*e.g.,* proprietary APIs) is necessary to understand the data and make efficient use of it in other applications and technologies. Because this information is routinely treated as confidential or proprietary, the developer's cooperation is required to enable uses of the EHI that go beyond the capabilities provided by the developer's technology. This includes the capability to export complete information sets and to migrate data in the event that a user decides to switch to a different technology.

Separate from these contractual and intellectual property issues, users may become ''locked in'' to a particular technology, HIE, or HIN for financial or business reasons. For example, many health care providers have invested significant resources to adopt EHR technologies—including costs for deployment, customization, data migration, and training—and have tightly integrated these technologies into their information management strategies, clinical workflows, and business operations. As a result, they may be reluctant to switch to other technologies due to the significant cost and disruption this would entail.

Another important driver of technological dependence is the ''network effects'' of health IT adoption, which are amplified by a reliance on technologies and approaches that are not standardized and do not enable seamless interoperability. Consequently, health care providers and other health IT users may gravitate towards and become reliant on the proprietary technologies, HIEs, or HINs that have been adopted by other individuals and entities with whom they have the greatest need to exchange EHI. These effects may be especially pronounced within particular product or geographic areas. For example, a HIN that facilitates certain types of exchange or transactions may be so widely adopted that it is a de facto industry standard. A similar phenomenon may occur within a particular geographic area once a critical mass of hospitals, physicians, or other providers adopt a particular EHR technology, HIE, or HIN.

In these and other analogous circumstances of reliance or dependence, there is a heightened risk that an actor's conduct will interfere with access, exchange, or use of EHI. To assist with compliance, we highlight the following common scenarios, based on our outreach to stakeholders, in which actors exercise control over key interoperability elements.[109]

- Health IT developers of certified health IT that provide EHR systems or other technologies used to capture EHI at the point of care are in a unique position to control subsequent access to and use of that information.
- HINs and HIEs may be in a unique position to control the flow of information among particular persons or for particular purposes, especially if the HIN or HIE has achieved significant adoption in a particular geographic area or for a particular type of health information use case.
- Similar control over EHI may be exercised by other entities, such as health IT developers of certified health IT, that supply or control proprietary technologies, platforms, or services that are widely adopted by a class of users or that are a ''de facto standard'' for certain types of EHI exchanges or transactions.
- Health care providers within health systems and other entities that provide health IT platforms, infrastructure, or information sharing policies may have a degree of control over interoperability or the movement of data within a geographic area that is functionally equivalent to the control exercised by a dominant health IT developer, HIN, or HIE.

To avoid violating the information blocking provision, actors with control over interoperability elements should be careful not to engage in practices that exclude persons from the use of those elements or create artificial costs or other impediments to their use.

We encourage comment on these and other circumstances that may present an especially high likelihood that a practice will interfere with access, exchange, or use of EHI within the meaning of the information blocking provision.

c. Examples of Practices Likely To Interfere With Access, Exchange, or Use of EHI

To further clarify the scope of the information blocking provision, below we describe several types of practices that would be likely to interfere with access, exchange, or use of EHI. These examples clarify and expand on those set forth in section 3022(a)(2) of the PHSA.

Because information blocking can take many forms, we emphasize that the categories of practices described below are illustrative only and do not provide an exhaustive list or comprehensive description of practices that may implicate the information blocking provision and its penalties. We also reiterate that to implicate the provision is not necessarily to violate it, and that each case will turn on its own unique facts. For instance, a practice that seemingly meets the statutory definition of information blocking would not be information blocking if it was required by law, if one or more elements of the definition were not met, or if it was covered by one of the proposed exceptions for certain reasonable and necessary activities detailed in section VIII.D of this preamble. For the purposes of the following discussion, we do not consider the applicability of any exceptions proposed in section VIII.D of this preamble; we therefore strongly encourage readers to review that section in conjunction with the discussion of practices in this section below.

i. Restrictions on Access, Exchange, or Use

The information blocking provision establishes penalties, including civil monetary penalties, or requires appropriate disincentives, for practices that restrict access, exchange, or use of EHI for permissible purposes. For example, section 3022(a)(2)(A) of the PHSA states that information blocking may include practices that restrict authorized access, exchange, or use for treatment and other permitted purposes under applicable law. Section 3022(a)(2)(C)(i) of the PHSA states that information blocking may include implementing health IT in ways that are likely to restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems.

One means by which actors may restrict access, exchange, or use of EHI is through formal restrictions. These may be expressed in contract or license terms, EHI sharing policies, organizational policies or procedures, or other instruments or documents that set forth requirements related to EHI or health IT. Additionally, in the absence of an express contractual restriction, an actor may achieve the same result by exercising intellectual property or other rights in ways that restrict access, exchange, or use. As an illustration, the following non-exhaustive examples illustrate types of formal restrictions that would likely implicate the information blocking provision. As stated above, the examples throughout this section VIII.C.5.c. are presented without consideration to whether a proposed exception applies, and readers are encouraged to familiarize themselves with section VIII.D of this preamble.

- A health system's internal policies or procedures require staff to obtain an individual's written consent before sharing any of a patient's EHI with unaffiliated providers for treatment purposes even though obtaining an individual's consent is not required by state or federal law.
- An EHR developer's software license agreement prohibits a customer from disclosing to its IT contractors certain technical interoperability information without which the customer and its IT contractors cannot efficiently export and convert EHI for use in other applications.
- A HIN's participation agreement prohibits entities that receive EHI through the HIN from transmitting that EHI to entities who are not participants of the HIN.
- An EHR developer sues to prevent a clinical data registry from providing interfaces to physicians who use the developer's EHR technology and wish to submit EHI to the registry. The EHR developer claims that the registry is infringing the developer's copyright in its database because the interface incorporates data mapping that references the table headings and rows of the EHR database in which the EHI is stored.

Access, exchange, or use of EHI can also be restricted in less formal ways. The information blocking provision would be implicated, for example, where an actor simply refuses to exchange or to facilitate the access or use of EHI, either as a general practice or in isolated instances. The refusal may be expressly stated, or it may be implied from the actor's conduct, as where the actor ignores requests to share EHI or provide interoperability elements; gives implausible reasons for not doing so; or insists on terms or conditions that are so objectively unreasonable that they amount to a refusal to provide access, exchange, or use of the EHI. Some examples of informal restrictions include, but are not limited to:

- A health IT developer of certified health IT refuses to license interoperability elements that are reasonably necessary for the developer's customers, their IT contractors, and other health IT developers to develop and deploy software that will work with the certified health IT.
- A health system incorrectly claims that the HIPAA Rules or other legal requirements preclude it from exchanging EHI with unaffiliated providers.

[109] As an important clarification, we note that control over interoperability elements may exist with or without the actor's ability to manipulate the price of the interoperability elements in the market.

- An EHR developer ostensibly allows third-party developers to deploy apps that are interoperable with its EHR system. However, as a condition of doing so, the third-party developers must provide their source code and grant the EHR developer the right to use it for its own purposes—terms that almost no developer would willingly accept.
- A provider notifies its EHR developer of its intent to switch to another EHR system and requests a complete export of its EHI. The developer will provide only the EHI in a PDF format, even though it already can and does produce the data in a commercially reasonable structured format.

We emphasize that restrictions on access, exchange, or use that are required by law would not implicate the information blocking provision. Moreover, we recognize that some restrictions, while not required by law, may be reasonable and necessary for the privacy and security of individuals' EHI; such practices may qualify for protection under the exceptions proposed in section VIII.D.2 and 3 of this preamble.

ii. Limiting or Restricting the Interoperability of Health IT

The information blocking provision includes practices that restrict the access, exchange, or use of EHI in various ways (*see* section 3022(a)(2) of the PHSA). These practices could include, for example, disabling or restricting the use of a capability that enables users to share EHI with users of other systems or to provide access to EHI to certain types of persons or for certain purposes that are legally permissible. In addition, the information blocking provision would be implicated where an actor configures or otherwise implements technology in ways that limit the types of data elements that can be exported or used from the technology. Other practices that would be suspect include configuring capabilities in a way that removes important context, structure, or meaning from the EHI, or that makes the data less accurate, complete, or usable for important purposes for which it may be needed. Likewise, implementing capabilities in ways that create unnecessary delays or response times, or that otherwise limit the timeliness of EHI accessed or exchanged, would interfere with the access, exchange, and use of that information and would therefore implicate the information blocking provision. We note that any conclusions regarding such interference would be based on fact-finding specific to each case and would need to consider the applicability of an exception.

We propose that the information blocking provision would be implicated if an actor were to deploy technological measures that limit or restrict the ability to reverse engineer the functional aspects of technology in order to develop means for extracting and using EHI maintained in the technology. This may include, for example, employing technological protection measures that, if circumvented, would trigger liability under the Digital Millennium Copyright Act (*see* 17 U.S.C. 1201) or other laws.

The following hypothetical situations illustrate some (though not all) of the types of practices described above and which would implicate the information blocking provision.

- A health system implements locally-hosted EHR technology certified to proposed § 170.315(g)(10) (the health system acts as an API Data Provider as defined by § 170.102). As required by proposed § 170.404(b)(2), the technology developer provides the health system with the capability to automatically publish its production endpoints (*i.e.,* the internet servers that an app must ''call'' and interact with in order to request and exchange patient data). The health system chooses not to enable this capability, however, and provides the production endpoint information only to apps it specifically approves. This prevents other applications—and patients that use them—from accessing data that should be made readily accessible via standardized APIs.
- A hospital directs its EHR developer to configure its technology so that users cannot easily send electronic patient referrals and associated EHI to unaffiliated providers, even when the user knows the Direct address and/or identity (*i.e.,* National Provider Identifier) of the unaffiliated provider.
- An EHR developer that prevents (such as by way of imposing exorbitant fees unrelated to the developer's costs, or by some technological means) a third-party clinical decision support (CDS) app from writing EHI to the records maintained by the EHR developer on behalf of a health care provider (despite the provider authorizing the third-party app developer's use of EHI) because the EHR developer: (1) Offers a competing CDS software to the third-party app; and (2) includes functionality (*e.g.,* APIs) in its health IT that would provide the third party with the technical capability to modify those records as desired by the health care provider.
- Although an EHR developer's patient portal offers the capability for patients to directly transmit or request for direct transmission of their EHI to a third party, the developer's customers (*e.g.,* health care providers) choose not to enable this capability.
- A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider, but takes several days to respond.

iii. Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

The information blocking provision encompasses practices that create impediments to innovations and advancements to the access, exchange, and use of EHI, including care delivery enabled by health IT (section 3022(a)(2)(C)(ii) of the PHSA). Importantly, the information blocking provision would be implicated and penalties may apply if an actor were to engage in exclusionary, discriminatory, or other practices that impede the development, dissemination, or use of interoperable technologies and services that enhance access, exchange, or use of EHI.

Most acutely, the information blocking provision would be implicated if an actor were to refuse to license or allow the disclosure of interoperability elements to persons who require those elements to develop and provide interoperable technologies or services—including those that might complement or compete with the actor's own technology or services. The same would be true if the actor were to allow access to interoperability elements but were to restrict their use for these purposes. The following examples, which are not exhaustive, illustrate practices that would likely implicate the information blocking provision by interfering with access, exchange, or use of EHI:

- A health IT developer of certified health IT refuses to license an API's interoperability elements, to grant the rights necessary to commercially distribute applications that use the API's interoperability elements, or to provide the related services necessary to enable the use of such applications in production environments.
- An EHR developer of certified health IT requires third-party applications to be ''vetted'' for security before use but does not promptly conduct the vetting or conducts the vetting in a discriminatory or exclusionary manner.
- A health IT developer of certified health IT refuses to license interoperability elements that other software applications require to efficiently access, exchange, and use

EHI maintained in the developer's technology.

Rather than restricting interoperability elements, an actor may insist on terms or conditions that are burdensome and discourage their use. These practices would implicate the information blocking provision for the reasons described above. Consider the following non-exhaustive examples:

- An EHR developer of certified health IT maintains an ''app store'' through which other developers can have ''apps'' listed that run natively on the EHR developer's platform. However, if an app ''competes'' with the EHR developer's apps or apps it plans to develop, the developer *requires* that the app developer grant the developer the right to use the app's source code.
- A health care provider engages a systems integrator to develop an interface engine. However, the provider's license agreement with its EHR developer prohibits it from disclosing technical documentation that the systems integrator needs to perform the work. The EHR developer states that it will only permit the systems integrator to access the documentation if all of its employees sign a broad non-compete agreement that would effectively bar them from working for any other health IT companies.

The information blocking provision would be implicated also if an actor were to discourage efforts to develop or use interoperable technologies or services by exercising its influence over customers, users, or other persons, as in the following non-exhaustive examples:

- An EHR developer of certified health IT maintains an ''app store'' through which other developers can have ''apps'' listed that run natively on the EHR developer's platform. The EHR developer charges app developers a substantial fee for this service unless an app developer agrees not to deploy the app in any other EHR developers' app stores.
- A hospital is working with several health IT developers to develop an application that will enable ambulatory providers who use different EHR systems to access and update patient data in the hospital's EHR system from within their ambulatory EHR workflows. The inpatient EHR developer, being a health IT developer of certified health IT, pressures the hospital to abandon this project, stating that if it does not it will no longer receive the latest updates and features for its inpatient EHR system.
- A health IT developer of certified health IT discourages customers from procuring data integration capabilities from a third-party developer, claiming that it will be providing such capabilities free of charge in the next release of its product. In reality, the capabilities it is developing are more limited in scope and are still 12–18 months from being production-ready.
- A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians that do not comply.

Similar concerns would arise were an actor to engage in discriminatory practices—such as imposing unnecessary and burdensome administrative, technical, contractual, or other requirements on certain persons or classes of persons—that interfere with access and exchange or EHI by frustrating or discouraging efforts to enable interoperability. The following non-exhaustive examples illustrate some ways this could occur:

- An HIN charges additional fees, requires more stringent testing or certification requirements, or imposes additional terms for participants that are competitors, are potential competitors, or may use EHI obtained via the HIN in a way that facilitates competition with the HIN.
- A health care provider imposes one set of fees and terms to establish interfaces or data sharing arrangements with several registries and exchanges, but offers another more costly or significantly onerous set of terms to establish substantially similar interfaces and arrangements with an HIE or HIN that is used primarily by health plans that purchase health care services from the provider at negotiated reduced rates.
- A health IT developer of certified health IT charges customers fees, throttles speeds, or limits the number of records they can export when exchanging EHI with a regional HIE that supports exchange among users of competing health IT products, but does not impose like fees or limitations when its customers exchange EHI with enterprise HIEs that primarily serve users of the developer's own technology.
- As a condition of disclosing interoperability elements to third-party developers, an EHR developer requires third-party developers to enter into business associate agreements with all of the EHR developer's covered entity customers, even if the work being done is not for the benefit of the covered entities.
- A health IT developer of certified health IT takes significantly longer to provide or update interfaces that facilitate the exchange of EHI with users of competing technologies or services.

We clarify that not all instances of differential treatment would necessarily constitute a discriminatory practice that implicates the information blocking provision. For example, different fee structures or other terms may reflect genuine differences in the cost, quality, or value of the EHI and the effort required to provide access, exchange, or use. We also note that, in certain circumstances, it may be reasonable and necessary for an actor to restrict or impose reasonable and non-discriminatory terms or conditions on the use of interoperability elements, even though such practices could implicate the information blocking provision. For this reason, we propose in section VIII.D.6 of this preamble to establish a narrow exception that would apply to these types of practices.

iv. Rent-Seeking and Other Opportunistic Pricing Practices

Certain practices that artificially increase the cost and expense associated with accessing, exchanging, and using EHI will implicate the information blocking provision. Such practices are plainly contrary to the information blocking provision and the concerns that motivated its enactment.

An actor may seek to extract profits or capture revenue streams that would be unobtainable without control of a technology or other interoperability elements that are necessary to enable or facilitate access, exchange, or use of EHI. As discussed in section VIII.C.5.b.iii of this proposed rule, most EHI is currently stored in EHRs and other source systems that use proprietary data models or formats; this puts EHR developers (and other actors that control data models or standards) in a unique position to block access to (including the export and portability of) EHI for use in competing systems or applications, or to charge rents for access to the basic technical information needed to accomplish the access, exchange, or use of EHI for these purposes. These information blocking concerns may be compounded to the extent that EHR developers do not disclose, in advance, the fees they will charge for interfaces, data export, data portability, and other interoperability-related services (*see* 80 FR 62719; 80 FR 16880–81). We note that these concerns are not limited to EHR developers. Other actors who exercise substantial control over EHI or essential interoperability elements may engage in analogous behaviors that would implicate the information blocking provision.

To illustrate, we provide the following non-exhaustive examples, which reflect some of the more common types of rent-seeking and opportunistic behaviors of which we are aware and that are likely to interfere with access, exchange, or use of EHI:

- An EHR developer of certified health IT charges customers a fee to provide interfaces, connections, data export, data conversion or migration, or other interoperability services, where the amount of the fee exceeds the actual costs that the developer reasonably incurred to provide the services to the particular customer(s).
- An EHR developer of certified health IT charges a fee to perform an export using the EHI export capability proposed in § 170.315(b)(10) for the purposes of switching health IT systems or to provide patients access to EHI.
- An EHR developer of certified health IT charges more to export or use EHI in certain situations or for certain purposes, such as when a customer is transitioning to a competing technology or attempting to export data for use with a HIE, third-party application, or other technology or service that competes with the revenue opportunities associated with the EHR developer's own suite of products and services.
- An EHR developer of certified health IT interposes itself between a customer and a third-party developer, insisting that the developer pay a licensing fee, royalty, or other payment in exchange for permission to access the EHR system or related documentation, where the fee is not reasonably necessary to cover any additional costs the EHR developer incurs from the third-party developer's activities.
- An analytics company provides services to the customers of an EHR developer of certified health IT, including de-identifying customer EHI and combining it with other data to identify areas for quality improvement. The EHR developer insists on a revenue sharing arrangement whereby it would receive a percentage of the revenue generated from these activities in return for facilitating access to its customers' EHI, which turns out to be disadvantageous to customers. The revenue the EHR developer would receive exceeds its reasonable costs of facilitating the access to EHI.

The information blocking provision would clearly be implicated by these and other practices by which an actor profits from its unreasonable control over EHI or interoperability elements without adding any efficiency to the health care system or serving any other procompetitive purpose. But the reach of the information blocking provision is not limited to these types of practices. We interpret the definition of information blocking to encompass *any* fee that materially discourages or otherwise imposes a material impediment to access, exchange, or use of EHI. We use the term ''fee'' in the broadest possible sense to refer to any present or future obligation to pay money or provide any other thing of value and propose to include this definition in § 171.102. We believe this scope may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services. Therefore, as discussed in section VIII.D.4 of this preamble, we propose to create an exception that, subject to certain conditions, would permit the recovery of costs that are reasonably incurred to provide access, exchange, and use of EHI. We refer readers to that section for additional details regarding this proposal.

v. Non-Standard Implementation Practices

Section 3022(a)(2)(B) of the PHSA states that information blocking may include implementing health IT in non-standard ways that substantially increase the complexity or burden of accessing, exchanging, or using EHI. In general, this type of interference is likely to occur when, despite the availability of generally accepted technical, policy, or other approaches that are suitable for achieving a particular implementation objective, an actor does not implement the standard, does not implement updates to the standard, or implements the standard in a way that materially deviates from its formal specifications. These practices lead to unnecessary complexity and burden, such as the additional cost and effort required to implement and maintain ''point-to-point'' connections, custom-built interfaces, and one-off trust agreements.

While each case will necessarily depend on its individual facts, and while we recognize that the development and adoption of standards across the health IT industry is an ongoing process, we propose that the information blocking provision would be implicated in at least two distinct sets of circumstances. First, information blocking may arise where an actor chooses not to adopt, or to materially deviate from, relevant standards, implementation specifications, and certification criteria adopted by the Secretary under section 3004 of the PHSA. Second, even where no federally adopted or identified standard exists, if a particular implementation approach has been broadly adopted in a relevant industry segment, deviations from that approach would be suspect unless strictly necessary to achieve substantial efficiencies.

To further illustrate these types of practices that would implicate the information blocking provision, we provide the following non-exhaustive examples of conduct that would be likely to interfere with access, exchange, or use of EHI:

- An EHR developer of certified health IT implements the C–CDA for receiving transitions of care summaries but only sends transitions of care summaries in a proprietary or outmoded format.
- A health IT developer of certified health IT adheres to the ''required'' portions of a widely adopted industry standard but chooses to implement proprietary approaches for ''optional'' parts of the standard when other interoperable means are readily available.

Even where no standards exist for a particular purpose, actors should not design or implement health IT in non-standard ways that unnecessarily increase the costs, complexity, and other burden of accessing, exchanging, or using EHI. For example, an EHR developer of certified health IT designs its database tables in a way that is unreasonably difficult to ''map'' to a non-proprietary format, which is a necessary prerequisite to converting the EHI to a format that can be used in other software applications. When a customer requests the capability to export EHI to a clinical data registry, the EHR developer quotes substantial costs resulting from the need to write custom code to enable this functionality. Based on these facts, the fees do not reflect costs that are reasonably incurred to provide the service and are instead the result of the developer's impractical design choices. We are aware that some actors attribute certain non-standard implementations on legacy systems that the actor did not themselves design but which have to be integrated into the actor's health IT. Such instances will be considered on a case by case basis.

Again, we reiterate that information blocking can take many forms and that the practices (and categories of practices) described above do not provide an exhaustive list or comprehensive description of practices that may implicate the information blocking provision.

6. Applicability of Exceptions

a. Reasonable and Necessary Activities

As discussed above, section 3022(a)(3) authorizes the Secretary to identify, through notice and comment rulemaking, reasonable and necessary *activities* that do not constitute information blocking for purposes of the definition set forth in section 3022(a)(1). Separately, the Cures Act identifies at section 3022(a)(1) *practices* that contravene the definition of information blocking. Following this Cures Act terminology, conduct that implicates the information blocking provision and that does not fall within one of the exceptions described in section VIII.D of this preamble, or does not meet all conditions for an exception, would be considered a ''practice.'' Conduct that falls within an exception and meets all the applicable conditions for that exception would be considered an ''activity.'' The challenge with this distinction is that when examining conduct that is the subject of an information blocking claim— an actor's actions that likely interfered with access, exchange, or use of EHI—it can be illusory to distinguish, on its face, conduct that is a *practice* and conduct that is an *activity.* Indeed, conduct that implicates the information blocking provision but falls within an exception could nonetheless be considered information blocking in the event that the actor has not satisfied the conditions applicable to that exception.

While we acknowledge the terminology used in the Cures Act, we propose to use the term ''practice'' throughout this proposed rule when we describe conduct that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information, regardless of whether that conduct meets the conditions for an exception to the information blocking provision. Consistent with this approach, when identifying reasonable and necessary activities in §§ 171.200 through 171.206, we describe *practices* that, if all the applicable conditions are met, are reasonable and necessary and not information blocking. We have taken this approach, in part, because we believe that to adopt the terminology of activity to describe conduct that may or may not be information blocking would confuse the reader and obfuscate our intent in certain circumstances. As an illustration, a health care provider may implement an organizational security policy that limits access, exchange, or use of certain information to certain users (*e.g.,* role-based access). Prior to determining whether the implementation of the security policy is reasonable and necessary under the circumstances, such conduct would be considered a ''practice'' that implicates the information blocking provision. However, it may later be determined that such conduct is reasonable and necessary and would then be considered an ''activity.'' Due to these types of scenarios, we contend that the better approach is to use one term—practice— throughout the proposed rule and clarify when describing the conduct at issue whether it is a practice that is information blocking, a practice that implicates the information blocking provision, or a practice that is reasonable and necessary and not information blocking.

b. Treatment of Different Types of Actors

The proposed exceptions would apply to health care providers, health IT developers of certified health IT, HIEs, and HINs who engage in certain practices covered by an exception, provided that all applicable conditions of the exception are satisfied at all relevant times and for each practice for which the exception is sought. The exceptions are generally applicable to all actors. However, in some instances we propose conditions within an exception that apply to a particular type of actor.

c. Establishing That Activities and Practices Meet the Conditions of an Exception

We propose that, in the event of an investigation of an information blocking complaint, an actor must demonstrate that an exception is applicable and that the actor met all relevant conditions of the exception at all relevant times and for each practice for which the exception is sought. We consider this allocation of proof to be a substantive condition of the proposed exceptions. As a practical matter, we propose that actors are in the best position to demonstrate compliance with the conditions of the proposed exceptions and to produce the detailed evidence necessary to demonstrate that compliance. We request comment about the types of documentation and/or standardized methods that an actor may use to demonstrate compliance with the exception conditions.

D. Proposed Exceptions to the Information Blocking Provision

We propose to establish seven exceptions to the information blocking provision. The exceptions would apply to certain activities that may technically meet the definition of information blocking but that are reasonable and necessary to further the underlying public policies of the information blocking provision.

The seven proposed exceptions are based on three related policy considerations. First, each exception is limited to certain activities that clearly advance the aims of the information blocking provision. These reasonable and necessary activities include providing appropriate protections to prevent harm to patients and others; promoting the privacy and security of EHI; promoting competition and innovation in health IT and its use to provide health care services to consumers, and to develop more efficient means of health care delivery; and allowing system downtime in order to implement upgrades, repairs, and other changes to health IT. Second, each exception addresses a significant risk that regulated actors will not engage in these beneficial activities because of uncertainty concerning the breadth or applicability of the information blocking provision. Finally, each exception is subject to strict conditions to ensure that it is limited to activities that are reasonable and necessary.

The first three exceptions, set forth in VIII.D.1–D.3, extend to certain activities that are reasonable and necessary to prevent harm to patients and others; promote the privacy of EHI; and promote the security of EHI, subject to strict conditions to prevent the exceptions from being misused. We believe that without these exceptions, actors may be reluctant to engage in the types of reasonable and necessary activities described below, and that this could erode trust in the health IT ecosystem and undermine efforts to provide access and facilitate the exchange and use of EHI for important purposes. Such a result would be contrary to the purpose of the information blocking provision and the broader policies of the Cures Act.

The next three exceptions, set forth in VIII.D.4–D.6, address activities that are reasonable and necessary to promote competition and consumer welfare. First, we propose to permit the recovery of certain types of reasonable costs incurred to provide technology and services that enable access to EHI and facilitate the exchange and use of that information, provided certain conditions are met. Second, we propose to permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, subject to a duty to provide a reasonable alternative. And, third, we propose an exception that would permit an actor to license interoperability elements on reasonable and non-discriminatory terms. These exceptions would be subject to strict conditions to ensure that they do not extend protection to practices that raise information blocking concerns.

The last exception, set forth in VIII.D.7, recognizes that it may be reasonable and necessary for actors to make health IT temporarily unavailable for the benefit of the overall performance of health IT. This exception would permit an actor to make the operation of health IT unavailable in order to implement upgrades, repairs, and other changes.

As context for the exceptions proposed below in VIII.D.4–D.6, we note that addressing information blocking is critical for promoting competition and innovation in health IT and for the delivery of health care services to consumers. Indeed, the information blocking provision itself expressly addresses practices that impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health IT (section 3022(a)(2)(C)(ii) of the PHSA). As discussed in section VIII.C.5.b.iii of this preamble, health IT developers of certified health IT, HIEs, HINs, and, in some instances, health care providers may exploit their control over interoperability elements to create barriers to entry for competing technologies and services that offer greater value for health IT customers and users, provide new or improved capabilities, and enable more robust access, exchange, and use of EHI.[110] More than this, information blocking may harm competition not just in health IT markets, but also in markets for health care services.[111] Dominant providers in these markets may leverage their control over technology to limit patient mobility and choice.[112] They may also pressure independent providers to adopt expensive, hospital-centric technologies that do not suit their workflows, limit their ability to share information with unaffiliated providers, and make it difficult to adopt or use alternative technologies that could offer greater efficiency and other benefits.[113] The technological dependence resulting from these practices can be a barrier to entry by would-be competitors. It can also make independent providers vulnerable to acquisition or induce them into exclusive arrangements that enhance the market power of incumbent providers, while preventing the formation of clinically-integrated products and networks that offer more choice and better value to consumers and purchasers of health care services.

Section 3022(a)(5) of the PHSA provides that the Secretary may consult with the Federal Trade Commission (FTC) in defining practices that do not constitute information blocking because they are necessary to promote competition and consumer welfare. We appreciate the expertise and informal technical assistance of FTC staff, which we have taken into consideration in developing the exceptions described in VIII.D.4–D.6 of this preamble. We note that the language in the Cures Act regarding information blocking is substantively and substantially different from the language and goals in the antitrust laws enforced by the FTC. We view the Cures Act as authorizing ONC and OIG to regulate conduct that may be considered permissible under the antitrust laws. On this basis, this proposed rule requires that actors who control interoperability elements cooperate with individuals and entities that require those elements for the purpose of developing, disseminating, and enabling technologies and services that can interoperate with the actor's technology.

We emphasize that ONC is taking this approach because we view patients as having an overwhelming interest in EHI about themselves, and particularly observational health information (see the discussion in section VIII.C.4.b of this preamble). As such, access to EHI, and the EHI itself, should not be traded or sold by those actors who are custodians of EHI or who control its access, exchange, or use. We emphasize that such actors should not be able to charge fees for providing electronic access, exchange, or use of patients' EHI. We propose that actors should be required to share EHI unless they are prohibited from doing so under an existing law or are covered by one of the exceptions detailed in this preamble. In addition, any remedy sought or action taken by HHS under the information blocking provision would be independent from the antitrust laws and would not prevent FTC or DOJ from taking action with regard to the same actor or conduct.

We request comment on the following seven proposed exceptions, including whether they will achieve our stated policy goals.

1. Preventing Harm

We propose to establish an exception to the information blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. The exception and corresponding conditions are set forth in the proposed regulation text in § 171.201.

This proposed exception would acknowledge the public interest in protecting patients and other persons against unreasonable risks of harm that, in certain narrowly defined circumstances described below, justify practices that are likely to interfere with access, exchange, or use of EHI and that would implicate the information blocking provision in the absence of an exception.

The exception would be subject to strict conditions, which we believe are necessary to prevent patient safety from being used as a pretext for information blocking or as a post hoc rationalization for practices that are not reasonable and necessary to address material risks of harm to a patient or another person.

We have adopted the terminology of ''patient'' to denote the context in which the threat of harm arises. That is, this proposed exception has been designed to recognize certain practices taken for the benefit of recipients of health care—those individuals whose EHI is at issue—and other persons whose information may be recorded in that EHI or who may be at risk of harm because of the access, use, or exchange of EHI. The use of the term ''patient'' does not require, other than in the context of the risk of harm determined by a licensed health care professional (*see* § 171.201(a)(3)), that an actor seeking to benefit from this exception needs to have a clinician-patient relationship with the individual (or individuals) at risk of harm. Indeed, a health IT developer of certified health IT would be able to benefit from this exception in connection with practices undertaken for the benefit of individuals receiving (or having received, or expected to receive) care from a health care provider that uses the developer's health IT. Similarly, an HIE or HIN that exchanges or facilitates the exchange of EHI would

[110] *See also* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, *Making Health Care Markets Work: Competition Policy for Health Care,* 16–17 (Apr. 2017), available at *http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930.*

[111] *See, e.g.,* Keynote Address of FTC Chairwoman Edith Ramirez, Antitrust in Healthcare Conference Arlington, VA (May 12, 2016), *available at https://www.ftc.gov/system/files/documents/public_statements/950143/160519antitrusthealthcarekeynote.pdf.*

[112] *See, e.g.,* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, *Making Health Care Markets Work: Competition Policy for Health Care,* 16–17 (Apr. 2017), *available at http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930.*

[113] *See, e.g., Healthcare Research Firm Toughens Survey Standards as More CIOs Reap the Profits of Reselling Vendor Software,* Black Book, *available at http://www.prweb.com/releases/2015/02/prweb12530856.htm;* Arthur Allen, *Connecticut Law Bans EHR-linked Information Blocking, Politico.com* (Oct. 29, 2015).

be able to benefit from this exception in connection with the activities carried out by the HIE or HIN for or at the direction of a health care provider.

Patient Harm Risks That Would Be Cognizable Under This Exception

Consistent with the definition of information blocking, we have identified certain risks to patient harm that arise in the context of access, exchange, or use of EHI. To qualify for this proposed exception, an actor's practice must respond to a risk that is cognizable under this exception.

Risk of Corrupt or Inaccurate Data Being Recorded or Incorporated in a Patient's Electronic Health Record

The exception may apply to practices that prevent harm arising from corrupted or inaccurate EHI being recorded or incorporated in a patient's electronic health record. Users of health IT systems strive to maintain accurate electronic health records by carefully inputting EHI and verifying existing EHI. Occasionally a clinician or other user of health IT is presented with EHI that, due to a failure of the technology, is either entirely incorrect or contains inaccurate information. At other times, EHI could become corrupted. In these cases, the sharing or integration of such EHI could lead to inaccuracies in the patient's electronic health record that then run the risk of being propagated further. We note, however, that known inaccuracies in some data within a record may not be sufficient justification to withhold the entire record if the remainder of the patient's EHI could be effectively shared without also presenting the known incorrect or corrupted information as if it were trustworthy. Also, we would expect that once information is known to be inaccurate or corrupted, a health care provider holding that record would, for example, take action to cure the inaccuracy or corruption. We understand that in the ordinary course of practice, and consistent with professional and legal standards for clinical record keeping, health care providers take appropriate action to remediate known problems with EHI and restore a record as a whole to be safely usable, and therefore safely sharable.

This recognized risk is limited to corruption and inaccuracies caused by performance and technical issues affecting health IT. For example, this exception may be relevant if certified health IT were to incorrectly present an old and superseded version of a medication list, or when only partial copies of laboratory tests are being linked to a patient when the patient's record is exchanged. However, this recognized risk does not extend to purported accuracy issues arising from the incompleteness of a patient's electronic health record generally. Electronic health records, like the paper charts they replaced, are inevitably imperfect records. Many patients see multiple health care providers and so it is unlikely that any single health care provider's record will provide a complete picture of a patient's health. Some patients intentionally keep certain information secret even from their health care providers, and others fail to share potentially critical information with their health care providers because they forget to, or simply do not understand its clinical significance.

While the access, exchange, or use of EHI in these situations could give rise to the risk of harm if the EHI was relied on without qualification, such reliance does not accord with our understanding of clinical practice, as the risk of incompleteness resulting from patients having multiple providers, or from errors of omission by patients and their care providers, is not unique to electronic health records or their interoperable exchange. Therefore, the risk that the EHI a given health care provider holds for a given patient may not be a perfectly complete record of that patient's health or care will not be recognized as being sufficient to support an actor qualifying for this exception in the face of a claim of information blocking.

We also acknowledge that certain federal and state laws, such as 42 CFR part 2 and state medical record laws, require an actor to obtain an individual's written consent before sharing health information. However, we propose that an actor would not be able to benefit from this exception on the basis of a perceived risk arising from exchanging or providing access to EHI when the EHI exchanged or made accessible does not include certain information due to a patient's decision not to consent to its disclosure. For example, this exception would not recognize an actor's conduct in not providing access, exchange, or use of a patient's electronic health record on the basis that the patient's failure to consent to the disclosure of substance abuse treatment information made the patient's record incomplete and thus inaccurate.

Risk of Misidentifying a Patient or Patient's Electronic Health Information

The exception may apply to practices that are designed to promote data quality and integrity and support health IT applications properly identifying and matching patient records or EHI. Accurately identifying patients and correctly attributing their EHI to them is a complex task and involves layers of safeguards, including verification of a patient's identity, proper registration in health IT systems, physical identification such as wristbands, and usability and implementation decisions such as ensuring the display of a patient's name and date of birth on every screen of the patient's electronic chart. When a clinician or other health IT user may know or reasonably suspect that specific EHI in a patient's record is or may be misattributed, either within a local record or as received through EHI exchange, it would be reasonable for them to avoid sharing or incorporating the EHI that they know would, or reasonably suspect could, propagate errors in the patient's records and thus pose the attendant risks to the patient. As discussed below, an actor's response to this risk would need to be no broader than necessary to mitigate the risk of harm arising from the potentially misidentified record or misattributed data. A health IT developer of certified health IT could not, for example, refuse to provide a batch export on the basis that the exported records may contain a misidentified record. Similarly, a health care provider that identified that a particular piece of information had been misattributed to a patient would not be excused from exchanging or providing access to all other EHI about the patient that had not been misattributed.

Determination by a Licensed Health Care Professional That the Disclosure of EHI Is Reasonably Likely To Endanger Life or Physical Safety

The exception may permit certain restrictions on the disclosure of an individual's EHI in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person. This would include the situation where a covered entity elected not to treat a person as the personal representative of an individual in situations of potential abuse or endangerment, including in accordance with 45 CFR 164.502(g)(5). In certain cases, the clinician may have individualized knowledge stemming from the clinician-patient relationship that, for a particular patient and for that patient's circumstances, harm could result if certain EHI were shared or transmitted electronically. Consistent with the HIPAA Privacy Rule, a decision not to provide access, exchange, or use of EHI on this basis would be subject to any right that an affected individual is afforded under applicable federal or state laws to have the determination reviewed and potentially reversed.

We request comment on whether the categories of harm described above capture the full range of safety risks that might arise directly from accessing, exchanging, or using EHI. We also request comment on whether we should consider other types of patient safety risks related to data quality and integrity concerns, or that may have a less proximate connection to EHI but that could provide a reasonable and necessary basis for an actor to restrict or otherwise impede access, exchange, or use of EHI in appropriate circumstances. We ask that commenters provide detailed rationale for any suggested revisions to these categories, including additional conditions that may be necessary to ensure that the exception is tailored and does not extend protection to practices that are not reasonable and necessary to promote patient safety and that could present information blocking concerns.

Reasonable Belief That Practice Was Necessary to Directly and Substantially Reduce the Likelihood of Harm

To qualify for this exception, an actor must have had a reasonable belief that the practice or practices will directly and substantially reduce the likelihood of harm to a patient or another person. As discussed above, the type of risk must also be cognizable under this exception.

An actor could meet this condition in two ways.

Qualifying Organizational Policy

In most cases, we anticipate that the actor would demonstrate that the practices it engaged in were consistent with an organizational policy that was objectively reasonable and no broader than necessary for the type of patient safety risks at issue. In these circumstances, we propose that an actor's policy would need to satisfy the following requirements.

First, we propose that the policy must be in writing.

Second, it must have been developed with meaningful input from clinical, technical, and other appropriate staff or others who have expertise or insight relevant to the risk of harm that the policy addresses. This condition would not be met if, for example, a hospital imposed top-down information sharing policies or workflows established by the hospital's EHR developer and approved by hospital administrators without meaningful input from the medical staff, IT department, and front-line clinicians who would implement, and thus be affected by, the policy and are in the best position to gauge how effective it will be at mitigating patient safety risks.

Third, we propose that the policy must have been implemented in a consistent and non-discriminatory manner. As part of this condition, the actor must have taken reasonable steps to educate its directors, officers, employees, contractors, and authorized personnel on how to apply the policy and to provide appropriate oversight to ensure that the policy is not applied in an arbitrary, discriminatory, or otherwise inappropriate manner. This condition would not be met if, for example, a policy or practice were based on factors that lacked a direct and substantial correlation with the particular risk of harm at issue.

Last, we propose that the policy must have been be no broader than necessary for the specific risk or type of risk at issue. For example, as evidence that the policy is no broader than necessary, the policy would need to identify the relevant risks and follow an approach to mitigating those risks that is based on current patient safety evidence and best practices, supplemented by input from clinical, technical, and other staff or others who are in the best position to make judgments about the policy's effectiveness, as discussed above. Further evidence that the policy was no broader than necessary would be whether the actor considered alternative approaches and reasonably concluded that, under the circumstances, those approaches were either inadequate to address the identified risks of harm or would not have reduced the likelihood of interference with access, exchange, or use of EHI. For example, a tailored response to the existence of corrupted data would necessarily permit all uncorrupted EHI to continue to be accessed, used, and exchanged. This condition would not be met, for example, if an actor's policy imposed a blanket ban on the sharing of EHI with users of different technologies or with health care providers who are not part of a particular health system, HIE, or HIN.

Qualifying Individualized Finding

We recognize that some health care providers (such as small practices) may not have comprehensive and formal policies governing all aspects of EHI and patient safety. Additionally, even if an organizational policy exists, it may not anticipate all of the potential risks of harm that could arise in real-world clinical or production environments of health IT. In these circumstances, in lieu of demonstrating that a practice conformed to the actor's policies and that the policies met the conditions described above, the actor could justify the practice or practices directly by making a finding in each case, based on the particularized facts and circumstances, that the practice is necessary and no broader than necessary to mitigate the risk of harm. To do so, we propose that the actor would need to show that the practices were approved on a case-by-case basis by an individual with direct knowledge of the relevant facts and circumstances and who had relevant clinical, technical, or other appropriate expertise. Such an individual would need to reasonably conclude, on the basis of those particularized facts and circumstances and his/her expertise and best professional judgment, that the practice was necessary, and no broader than necessary, to mitigate the risk of harm to a patient or other persons.

We propose that a licensed health care professional's independent and individualized judgment about the safety of the actor's patients or other persons would be entitled to substantial deference under this proposed exception. So long as the clinician actually considered all of the relevant facts and determined that, under the particular circumstances, the practice was necessary to protect the safety of the clinician's patient or other person, we would not second-guess the clinician's judgment. To provide further clarity on this point, we provide the following illustration.

A clinician suspects that a patient is at risk of domestic abuse. The patient has recently visited the clinic for a pregnancy test, and tells the clinician that the potential father is not her current partner. The test returns a positive result. The clinician notes that in the patient's electronic health record, her partner has been given access to view her test results. The clinician, considering all factors for this particular situation and particular patient, and aware of the clinic's policy towards the restriction of electronic health information sharing, concludes that releasing this result electronically could place the patient at risk of harm. The clinician thus chooses not to release the test result electronically and plans to deliver the result to the patient in a safe manner. The exception would apply in this case because the clinician reasonably believes, based on the relationship with this particular patient and the clinician's best clinical judgment, that the restriction is necessary to prevent harm to the patient.

We seek public comment on whether this proposed exception is appropriate and adequately balances the interest of promoting access, exchange, and use of EHI with legitimate concerns about the risk of harm to patients and others. In addition to any other relevant issues, we specifically request feedback on whether the exception is broad enough to prevent harm to patients and others and, if not, what additional risks we should address should we finalize this proposal; and whether there are additional safeguards the Secretary should adopt in order to prevent practices that attempt to undermine the policy goal of the exception. We also seek comment on whether there are customary practices (*e.g.,* standards of care) that advance patient safety concerns but which actors do not, as a matter of practice, record in documented policies, and which should be taken into account when assessing the reasonableness of a practice under this exception.

2. Promoting the Privacy of EHI

We propose to establish an exception to the information blocking provision for practices that are reasonable and necessary to protect the privacy of an individual's EHI, provided certain conditions are met. The exception and corresponding conditions are set forth in the proposed regulation text in § 171.202. We note that any practice engaged in to protect the privacy of an individual's EHI must be consistent with applicable laws related to health information privacy, including the HIPAA Privacy Rule as applicable, as well as with other applicable laws and regulations, such as the HITECH Act, 42 CFR part 2, and state laws. This exception to the information blocking provision does not alter an actor's obligation to comply with these and other applicable laws.

We believe this exception is necessary to support basic trust and confidence in health IT infrastructure. Without this exception, there would be a significant risk that actors would share EHI in inappropriate circumstances, such as when an individual has taken affirmative steps to request that the EHI not be shared, or when an actor has been unable to obtain reasonable assurances as to an individual's identity.

In contrast to the other exceptions defined in this proposed rule, this proposed exception has been structured with discrete ''sub-exceptions.'' An actor's practice must qualify for a sub-exception in order to be covered by this exception. The sub-exceptions have, to a large extent, been crafted to closely mirror privacy-protective practices that are recognized under state and federal privacy laws. In this way, the privacy sub-exceptions to the information blocking provision would recognize as reasonable and necessary practices that are engaged in by actors consistent with privacy laws, provided that certain conditions are met. We have proposed four sub-exceptions that address the following privacy protective practices: (1) Not providing access, exchange, or use of EHI when a state or federal law requires that a condition be satisfied before an actor provides access, exchange, or use of EHI, and the condition is not satisfied (proposed in § 171.202(b)); (2) not providing access, exchange, or use of EHI when the actor is a health IT developer of certified health IT that is not covered by the HIPAA Privacy Rule in respect to a practice (proposed in § 171.202(c)); (3) a covered entity, or a business associate on behalf of a covered entity, denying an individual's request for access to their electronic PHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3) (proposed at § 171.202(d)); and (4) not providing access, exchange, or use of EHI pursuant to an individual's request, in certain situations (proposed in § 171.202(e)). The rationale for each sub-exception is described in detail below.

An actor would need to satisfy at least one sub-exception in order that a purportedly privacy-protective practice that interferes with access, exchange, or use of EHI not be subject to the information blocking provision. Each sub-exception has conditions that must be met in order that an actor's practice qualifies for protection under the sub-exception.

Specific Terminology Used for the Purposes of This Proposed Exception

We note that this proposed exception and our discussion below uses certain terms that are defined by the HIPAA Rules[114] but that, for purposes of this exception, may have a broader meaning in the context of the information blocking provision and its implementing regulations as set forth in this Proposed Rule. In general, the terms ''access,'' ''exchange,'' and ''use'' have the meaning explained in section VIII.C.4.a of this preamble. However, in some instances we refer to ''use'' in the context of a disclosure or use of ePHI under the HIPAA Privacy Rule, in which case we have explicitly stated that the term ''use'' has the meaning defined in 45 CFR 160.103. Similarly, we refer in a few cases to an individual's right of access under 45 CFR 164.524, in which case the term ''access'' should be understood in that HIPAA Privacy Rule context. For purposes of section 3022 of the PHSA, however, the term ''access'' includes, but is broader than, an individual's access to their PHI as provided for by the HIPAA Privacy Rule (see section VIII.C.4.a of this preamble).

Finally, the term ''individual'' is defined by the HIPAA Rules at 45 CFR 160.103. Separately, under the information blocking enforcement provision, the term ''individual'' is used to refer to actors that are health IT developers of certified health IT, HINs, or HIEs, (*see* section 3022(b)(2)(A) of the PHSA). For purposes of this exception (and only this exception), we use neither of these definitions. Instead, the term ''individual'' encompasses any or all of the following: (1) An individual defined by 45 CFR 160.103; (2) a person who is the subject of EHI that is being accessed, exchanged or used; (3) a person who legally acts on behalf of an individual or person described in (1) or (2), including as a personal representative, in accordance with 45 CFR 164.502(g); or (4) a legal representative authorized to make health care decisions on behalf of a person or an executor or administrator who can act on behalf of the deceased's estate under state or other law.

We clarify that (2) varies from (1) because there could be individuals who could be the subject of EHI that is being accessed, exchanged, or used under (2), but who would not be the subject of PHI under (1). The purpose of (2) is to include EHI that would be accessed, exchanged or used by entities that are not subject to HIPAA (*e.g.,* non-covered entities and non-business associates). These entities could include, for example, health IT developers or data analytics companies that have access to EHI, but are not business associates.

We also clarify that (3) encompasses a person with *legal* authority to act on behalf of the individual, which includes a person who is a personal representative as defined under the HIPAA Privacy Rule. We included the component of *legal* authority to act in (3) because the HIPAA Privacy Rule gives rights to parents or legal guardians in certain circumstances where they are not the ''personal representative'' for their child(ren). For instance, a non-custodial parent who has requested a minor child's medical records under a court-ordered divorce decree may have legal authority to act on behalf of the

[114] 45 CFR part 160 and subparts A, C, and E of part 164.

child even if he or she is not the child's ''personal representative.'' Further, in limited circumstances and if permitted under state law, a family member may have *legal* authority to act on behalf of a patient to make health care decisions in emergency situations even if that family member may not be the ''legal representative'' or ''personal representative'' of the patient.

We have adopted this specialized usage to ensure that this privacy exception extends protection to information about, and respects the privacy preferences of, *all* individuals, not only those individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates.

Interaction Between Information Blocking, the Exception for Promoting the Privacy of EHI, and the HIPAA Privacy Rule

Having consulted extensively with the HHS Office for Civil Rights (OCR), who enforce the HIPAA Privacy, Security and Breach Notification Rules, we have developed the information blocking provision to advance our shared goals of preventing information blocking for nefarious or self-interested purposes while maintaining and upholding existing privacy rights and protections for individuals. The proposed exception for promoting the privacy of EHI (also referred to as ''the privacy exception'') operates in a manner consistent with the framework of the HIPAA Privacy Rule. We designed these exceptions to ensure that individual privacy rights are not diminished as a consequence of the information blocking provision, and to ensure that the information blocking provision does not require the use or disclosure of EHI in a way that would not be permitted under the HIPAA Privacy Rule. Our intent is that the information blocking provision does not conflict with the HIPAA Privacy Rule. Indeed, the sub-exception proposed in § 171.202(d) reflects a policy judgment that an actor's denial of access to an individual consistent with the limited conditions for such denials that are described in the HIPAA Privacy Rule at 45 CFR 164.524(a)(1), (2), and (3) is reasonable under the circumstances. We believe this resolves any potential conflict between limitations on an individual's right of access under the HIPAA Privacy Rule and the information blocking provision.

We note that the information blocking provision may operate to require that actors provide access, exchange, or use of EHI in situations that HIPAA does not. This is because the HIPAA Privacy Rule permits, but does not require, covered entities to use and disclose ePHI in most circumstances. The information blocking provision, on the other hand, requires that an actor provide access to, exchange, or use of EHI unless they are prohibited from doing so under an existing law or are covered by one of the exceptions detailed in this preamble. To illustrate, the HIPAA Privacy Rule permits health care providers to exchange ePHI for treatment purposes, but does not require them to do so. Under the information blocking provision, unless an exception to information blocking applies, or the interference is required by law, a primary care provider would be required to exchange ePHI with a specialist who requests it to treat an individual who was a common patient of the provider and the specialist, even if the primary care provider offered patient care services in competition with the specialist's practice, or would usually refer its patients to another specialist due to an existing business relationship.

Promoting Patient Privacy Rights

As discussed above, the information blocking provision would not require that actors provide access, exchange, or use of EHI in a manner that is not permitted under the HIPAA Privacy Rule or other privacy laws. As such, the privacy-protective controls existing under HIPAA would not be weakened by the information blocking provision. Moreover, we have structured the privacy exception to ensure that actors can engage in reasonable and necessary practices that advance the privacy interests of individuals.

For example, we believe that, unless required by law, actors should not be compelled to share EHI against patients' wishes or without adequate safeguards out of a concern that restricting the access, exchange, or use of the EHI would constitute information blocking. This could seriously undermine patients' trust and confidence in the privacy of their EHI and diminish the willingness of patients, providers, and other entities to provide or maintain health information electronically in the first place. In addition, such outcomes would undermine and not advance the goals of the information blocking provision and be inconsistent with the broader policy goal of the Cures Act to facilitate trusted exchange of EHI. Trusted exchange requires not only that EHI be shared in accordance with applicable law, but also that it be shared in a manner that effectuates individuals' expressed privacy preferences. We note and discuss below that an individual's expressed privacy preferences will not be controlling in all cases. An actor will not be able to rely on an individual's expressed privacy preference in circumstances where the access, exchange, or use is required by law.

For these reasons, we propose that the proposed sub-exception in § 171.202(e) would generally permit an actor to give effect to individuals' expressed privacy preferences, including their desire not to permit access, exchange, or use of their EHI. For example, provided that corresponding conditions have been met, a health care provider could honor a patient's request not to share their EHI in circumstances in which the HIPAA Privacy Rule would permit (though not require) the provider to disclose the information, such as for treatment purposes. At the same time, however, we believe that the privacy exception must be tailored to ensure that protection of an individual's privacy is not used as a pretext for information blocking. Accordingly, we propose that this exception, which is discussed more fully below, would be subject to strict conditions.

Privacy Practices Required by Law

Because the information blocking provision excludes from the definition of information blocking practices that are required by law (section 3022(a)(1) of the PHSA), privacy-protective practices that are required by law do not implicate the information blocking provision and do not require coverage from an exception. For example, the HIPAA Privacy Rule requires that a covered entity must agree to the request of an individual to restrict disclosure of protected health information (PHI) about the individual to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and not otherwise required by law and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.[115] If an individual made such a request and met all requirements of the HIPAA Privacy Rule, the actor would be *required by law* not to exchange the individual's EHI to a health plan. In this situation, the actor's interference with access, exchange, or use would not be information blocking and as such, the actor would not need to benefit from this exception.

Practices that are ''required by law'' can be distinguished from other practices that an actor engages in pursuant to a privacy law, but which are not ''required by law.'' Such privacy laws are typically framed in a way that

[115] 45 CFR 164.522(a)(1)(vi).

conditions the making of a ''disclosure'' on the satisfying of specific conditions, but does not expressly require that the actor engage in a practice that interferes with access, exchange, or use of EHI. For example, the HIPAA Privacy Rule provides that a covered entity *may* use or disclose PHI in certain circumstances where the individual concerned has authorized the disclosure.[116] The effect of this requirement is that the covered entity should not use or disclose the PHI in the absence of an individual's authorization. However, because the requirement does not prohibit the actor from exchanging the EHI in all circumstances, the actor would be at risk of engaging in a practice that was information blocking unless an exception applied. For this reason, we have included a sub-exception, addressed in § 171.202(b) and discussed below, that provides that an actor will not be engaging in information blocking if a state or federal privacy law imposes a precondition to the provision of access, exchange, or use, and that precondition has not been satisfied.

Sub-Exception To Proposed Privacy Exception: Precondition Not Satisfied

State and federal privacy laws that permit the disclosure of PHI often impose conditions that must be satisfied prior to a disclosure being made. We propose to establish a sub-exception to the information blocking provision that recognizes that an actor will not be engaging in information blocking if an actor does not provide access, exchange, or use of EHI because a necessary precondition required by law has not been satisfied. This exception will apply to all instances where an actor's ability to provide access, exchange, or use is ''controlled'' by a legal obligation to satisfy a condition, or multiple conditions, prior to providing that access, exchange, or use. To be covered by this exception, the actor must comply with conditions, which are discussed below.

The nature of the preconditions that an actor must satisfy in order to provide access, exchange, or use of EHI will depend on the privacy laws that regulate the actor. An actor that is regulated by a restrictive state privacy law may need to satisfy more conditions than an actor regulated by a less restrictive state privacy law, before providing access, exchange, or use. Similarly, certain state privacy laws may impose standards for meeting preconditions that are more rigorous than the laws in force elsewhere.

To illustrate how we propose this sub-exception would operate, we provide the following examples. We note that this list of examples is not exhaustive and that preconditions required by law that control access, exchange, or use of EHI that are not listed below would still qualify under this proposed sub-exception so long as all conditions are met.

- Certain federal and state laws require that a person provide consent before his or her EHI can be accessed, exchanged, or used for specific purposes. Although the HIPAA Privacy Rule does not have consent requirements for an individual (as that term is defined in the HIPAA Privacy Rule) when a covered entity or business associate is using or disclosing ePHI for treatment, payment or health care operations, some state laws and federal laws and regulations do require that a person's consent be obtained by the disclosing party/entity before disclosing certain health information. For example, for some sensitive health conditions such as HIV/AIDS, mental health, or genetic testing, state laws may impose a higher standard for disclosure of such information (*i.e.,* require consent) than is required under the HIPAA Privacy Rule. Additionally, under 42 CFR part 2, federally-assisted ''Part 2 programs'' generally are required to obtain a person's consent to disclose or re-disclose patient-identifying information related to the person's substance use disorder, such as treatment for addiction. The exception would operate to clarify an actor's compliance obligations in these situations. It would not be considered information blocking to refuse to provide access, exchange, or use of EHI if the actor has not received the person's consent, subject to conditions discussed herein.
- If an actor is required by law to obtain an individual's HIPAA authorization before providing access, exchange, or use of the individual's EHI, then the individual's refusal to provide an authorization would justify the actor's refusal to provide access, exchange, or use of EHI. The actor's refusal would, subject to conditions discussed herein, be protected under this exception.
- The HIPAA Privacy Rule, and many state privacy laws, authorize the disclosure of PHI in certain circumstances only once the identity and authority of the person requesting the information has been verified. We acknowledge that it is reasonable and necessary that actors take appropriate steps, consistent with federal and state laws, to ensure that EHI is not disclosed to the wrong person or to a person who is not authorized to receive it. Where an actor cannot verify the identity or authority of a person requesting access to EHI, and such verification is required by law before the actor can provide access, exchange, or use of the EHI, the actor's refusal to provide access, exchange, or use will, subject to the conditions discussed herein, be reasonable and necessary and will not be information blocking.
- Under the HIPAA Privacy Rule, a health care provider may share information with another health care provider for a quality improvement project if it has verified that the requesting entity has a relationship with the person whose information is being requested. Where the actor could not establish if the relationship existed, it would not be information blocking for the actor to refuse to provide access, exchange, or use, subject to the conditions discussed herein.

We seek comments generally on this proposed sub-exception. More specifically, we seek comment on how this proposed sub-exception would be exercised by actors in the context of state laws. We are aware that actors that operate across state lines or in multiple jurisdictions sometimes adopt organization-wide privacy practices that conform with the most restrictive privacy laws regulating their business. In order to ensure that the information blocking provision does not diminish the privacy rights of individuals being serviced by such actors, we are considering the inclusion of an accommodation in this sub-exception that would recognize an actor's observance of a legal precondition that the actor is required by law to satisfy in at least one state in which it operates. We believe this approach would be consistent with practices already in place for multi-state health care systems. For example, some states require specific consent requirements before exchanging sensitive health information such as a patient's mental health condition. As a result, the health care system will utilize one consent form for multi-jurisdiction purposes in order to meet various federal and state law requirements. However, in the event that we did adopt such an accommodation, we would also need to carefully consider how to ensure that before the use of the most stringent restriction is applied in all jurisdictions, the actor has provided all privacy protections afforded by that law across its entire business. This type of approach would ensure that an actor cannot take advantage of a more-restrictive privacy law for the benefit of this exception while not also fulfilling

[116] 45 CFR 164.508 (Uses and disclosures for which an authorization is required).

the privacy-protective obligations of the law being relied on. We seek comment on whether there is a need for ONC to adopt such an accommodation for actors operating in multiple states, and encourage commenters to identify any additional conditions that should attach to the provision of such an accommodation. We also request comment on our proposed approach to dealing with varying state privacy laws throughout this proposed sub-exception.

We also recognize that under the patchwork of state privacy laws, some states have enacted laws that more comprehensively identify the circumstance in which an individual or entity can and cannot provide access, exchange, or use of EHI. We are considering to what extent health care providers that are not regulated by the HIPAA Privacy Rule, and would rely instead on state laws for this sub-exception, would be able to benefit from this sub-exception when engaging in practices that interfere with access, exchange, or use of EHI for the purpose of promoting patient privacy. We seek comment on any challenges that may be encountered by health care providers that are not regulated as covered entities under the HIPAA Privacy Rule when seeking to take advantage of this proposed sub-exception. We also seek comment on whether there exists a class of health care provider that is not regulated by *any* federal or state privacy law that prescribes preconditions that must be satisfied in connection with the disclosure of EHI, and whether any such class of health care provider would benefit from a sub-exception similar to that proposed in § 171.202(c) for health IT developers of certified health IT.

Conditions To Be Met To Qualify for the Sub-Exception

In most circumstances, an actor would be in a position to influence whether a precondition is satisfied. For example, an actor could deprive a person of the opportunity to take some step that is a prerequisite for the exchange of their EHI, could assume the existence of a fact prejudicial to the granting of access without seeking to discover the truth or otherwise of the fact, or could make a determination that a precondition was not satisfied without properly informing itself of all relevant information. As such, we propose that this exception would be subject to conditions that ensure that the protection of an individual's privacy is not used as a pretext for information blocking.

We propose that an actor can qualify, in part, for this sub-exception by implementing and conforming to organizational policies and procedures that identify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order to satisfy the precondition. Most actors are covered entities or business associates for the purposes of the HIPAA Privacy Rule, and are already required to have policies and procedures and training programs in place that address how PHI and ePHI is used (as that term is defined in 45 CFR 160.103, as amended) and disclosed. As such, we expect that the overwhelming majority of actors will already be in a position to meet this condition, or would be able to meet this condition with modest additional effort. However, we acknowledge that some actors may not, for whatever reason, have privacy policies and practices in place, or may have implemented privacy policies and practices that do not sufficiently address the criteria to be used, and steps to be taken, to satisfy a precondition relied on by the actor. As such, we propose to provide an alternative basis on which to qualify, in part, for this sub-exception. We propose to permit actors to instead document, on a case-by-case basis, the criteria used by the actor to determine when the precondition will be satisfied, any criteria that were not met, and the reason why the criteria were not met. These alternative conditions, which are discussed in detail below, ensure that this sub-exception does not protect practices that are post hoc rationalizations used to justify improper practices, whilst also ensuring that actors do not face any pressure to disclose EHI in the situation where they do not have privacy policies and practices in place, or where their privacy policies and practices do not respond to the requirements of this condition.

Separately, we propose that if the precondition that an actor purports to have been satisfied relies on the provision of a consent or authorization from an individual, it is a condition of this sub-exception that the actor must have done all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide that consent or authorization.

We reiterate, again, that the information blocking provision does not require the provision of access, exchange, or use of EHI in a manner that would not be permitted under the HIPAA Privacy Rule.

Organizational Policies and Procedures

If an actor seeks to qualify for this sub-exception, in part, by implementing and conforming to organizational policies and procedures, such policies and procedures must be in writing, and specify the criteria to be used by the actor, and, if applicable, the steps that the actor will take, in order to satisfy the precondition relied on by the actor not to provide access, exchange, or use of EHI. It would not be sufficient for an actor to simply identify the existence of the precondition in their organizational policies and procedures.

We acknowledge that certain preconditions may be outside the direct control of the actor. For example, the requirement that an actor receive a valid authorization before releasing EHI in certain circumstances would be a precondition to be satisfied by the individual, and the actor may have little ability to influence the nature of the authorization that it receives. For preconditions of this nature, the actor's policies and procedures would only need to identify the criteria that the actor will apply and the steps that the actor will take to facilitate the satisfaction of the precondition, such as identifying the requirements for a valid authorization and the follow up steps (if any) to be taken in response to receipt of an authorization that does not meet those requirements. In contrast, where the satisfaction of a precondition relies solely on an actor, such as the ''minimum necessary'' determination made by HIPAA covered entities (or their business associates) when exchanging EHI that is ePHI, the actor's policies and procedures would need to particularize the steps that the actor will take in order to ensure that it satisfies the precondition. Where the precondition falls somewhere in between and relies on actions taken by both the actor and an individual, the actor's policies and procedures would need to address how the actor would do the things necessary within its control, which would include the steps it should take to facilitate all actions needed to be taken by an individual.

Take, for example, the situation where an actor needed to determine whether the subject individual had a relationship with a requesting entity as a precondition to exchanging EHI. The actor's policies and practices should, at minimum, identify the criteria to be applied, being the evidence that the actor would need in order to satisfy itself of the existence of a relationship, such as receipt of a Medicare or other insurance number, or other indicia of a relationship such as the establishment of a doctor-patient relationship.

An actor would only be eligible to benefit from this sub-exception if it has followed its processes and policies. Continuing the above example, an actor that chose not to provide access to EHI on the basis that insufficient evidence had been provided to establish the existence of the relationship, would need to show that its decision was based on the applicable criteria specified in the actor's policy and practices.

Using a different example, and as discussed above, the HIPAA Privacy Rule generally requires covered entities (and their business associates) to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.[117] Satisfying the ''minimum necessary'' requirement is a precondition to be met under the HIPAA Privacy Rule before an actor exchanges ePHI for many purposes. The determination of what constitutes the ''minimum necessary'' is a fact based judgment made by an actor. To allow covered entities the flexibility to address their unique circumstances, the HIPAA Privacy Rule requires covered entities (and their business associates) to make their own assessment of what ePHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce. To qualify for this proposed sub-exception, the actor's privacy policies and procedures would need to identify criteria for making a ''minimum necessary'' determination for both routine and non-routine disclosures and requests, including identifying the circumstances under which disclosing the entire medical record is reasonably necessary. For actors that are covered entities or business associates, the development of policies and procedures for the making of minimum necessary determinations for requesting, using and disclosing PHI is already a requirement of the HIPAA Privacy Rule, so we expect that actors will already have such policies and procedures in place. If an actor implemented its organizational policies and procedures for making ''minimum necessary'' determinations consistent with the HIPAA Privacy Rule, and otherwise met the other conditions of this exception, a decision to exchange the minimum necessary information but less information than requested by another entity would satisfy this sub-exception and not be considered information blocking.

Finally, an actor's policies and procedures must be implemented. This ensures that an actor can only satisfy this condition by reference to privacy policies and practices that individuals in fact benefit from, and not by policies and procedures that have been documented but not applied. Proper implementation would involve making the policies and processes available to all decision makers, and facilitating workforce and contractor understanding and consistent implementation of the actor's policies and procedures such as by providing training. This condition ensures that this sub-exception does not protect practices that are post hoc rationalizations used to justify improper practices.

As discussed above, to the extent existing state and federal laws apply to a given actor, we expect an actor to already have procedures in place to address those legal requirements. Indeed, the HIPAA Privacy Rule requires that covered entities have policies and procedures and training programs in place that address how PHI and ePHI are used (as those terms are defined in 45 CFR 160.103) and disclosed. Moreover, this exception is only enlivened when an actor asserts that its conduct was carried out to satisfy a precondition, and we expect that such conduct should be considered and deliberate.

We seek comment on this proposed condition generally, and specifically, on whether an actor's organizational policies and procedures provide a sufficiently robust and reliable basis for evaluating the bona fides, reasonableness, and necessity of practices engaged in to satisfy preconditions required by state or federal privacy laws.

Documenting Criteria and Rationale

If an actor's practice does not conform to an actor's organizational policies and procedures as required by § 171.202(b)(1), we propose that that an actor can seek to qualify for this sub-exception, in part, by documenting how it reached its decision that it would not provide access, use, or exchange of EHI on the basis that a precondition had not been satisfied. Such documentation must be created on a case-by-case basis. An actor will not satisfy this condition if, for instance, it sought to document a general practice that it had applied to all instances where the precondition had not been satisfied. Rather, the record created by the actor must address the specific circumstances of the specific practice (or interference) at issue.

The record created by the actor must identify the criteria used by the actor to determine when the precondition is satisfied. That is, it must identify the objective criteria that the actor applied to determine whether the precondition had been satisfied. Consistent with the condition to this sub-exception that the practice must be tailored to the privacy interest at issue (discussed below), those criteria would need to be directly relevant to satisfying the precondition. For example, if the precondition at issue was the provision of a valid HIPAA authorization, the actor's documented record should reflect, at minimum, that the authorization would need to meet each of the requirements specified for a valid authorization at 45 CFR 164.508(c). The record would then need to document the criteria that had not been met, and the reason so. Continuing the example, the actor could record that the authorization did not contain the name or other specific identification of the person making the request because the authorization only disclosed the person's first initial rather than first name, and the actor had records about multiple people with that same initial and last name.

We believe that this condition will provide the transparency necessary to demonstrate whether the actor has satisfied the conditions applicable to this exception. Moreover, it will ensure that a decision to not provide access, exchange, or use of EHI is considered and deliberate, and therefore reasonable and necessary.

We seek comment on this proposed condition.

Meaningful Opportunity To Provide Consent or Authorization

If the precondition that an actor purports to have satisfied relies on the provision of a consent or authorization from an individual, it is a condition of this sub-exception that the actor must have done all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide that consent or authorization. This condition will be relevant when, for example, a state privacy law or the HIPAA Privacy Rule requires an individual to provide their consent and/or HIPAA authorization before identifiable information can be accessed, exchanged, or used for specific purposes. For instance, a state law may require that an individual provide consent before a hospital can share her treatment information electronically with another treating health care provider. Under this scenario, the hospital's refusal to exchange the EHI in the absence of the individual's consent would be reasonable and necessary and would not be information blocking, so long as the hospital had provided the individual with a meaningful opportunity to provide that consent and where the criteria and other conditions of this proposed exception were met.

[117] 45 CFR 164.502(b).

In the context of the provision of consent, a meaningful opportunity would ordinarily require that an actor provide the individual with a legally compliant consent form; make a reasonable effort to inform an individual that she has the right to consent to the disclosure of her EHI; and provide the individual with sufficient information and educational material (commensurate with the circumstances of the disclosure). It would be best practice for an actor to also inform the individual about the revocability of any consent given, if and as provided in the relevant state or federal privacy law, and the actor's processes for acting on any revocation.

We are considering addressing this condition in further detail, whether by way of additional guidance or in regulation text. To this end, we seek comments regarding what actions an actor should take, within the actor's control, to provide an individual with a meaningful opportunity to provide a required consent or authorization, and whether different expectations should arise in the context of a consent versus a HIPAA authorization. For example, commenters may wish to provide comment on the actions to be taken to ensure that an individual has a meaningful opportunity to satisfy a precondition that the individual provide a HIPAA authorization. Specifically, in the context of a requirement that the authorization be signed, what effort should be expected from actors in seeking signatures from: (i) Persons acting for the patient where the patient is unable to sign a form; (ii) former patients whose EHI is being requested from third parties; or (iii) patients that are not in a facility, such as patients of individual physicians?

We clarify that after providing the individual with a meaningful opportunity to consent or provide authorization, we believe that it is the individual's responsibility to complete any required documentation before an actor is able to access, exchange, or use the individual's EHI. We do not expect the actor to ''chase'' the individual despite using its best efforts provide the individual with an opportunity to sign a consent or authorization form. So long as the actor has provided the individual with a meaningful opportunity to consent, the actor will have fulfilled this aspect of the eligibility requirements of this sub-exception.

Separately, to qualify for this sub-exception, to the extent that the precondition at issue was the provision of a consent or authorization by an individual, the actor must not have improperly encouraged or induced the individual to not provide the consent or authorization. This does not mean that the hospital cannot inform an individual about the advantages and disadvantages of exchanging EHI and any associated risks, so long as the information communicated is accurate and legitimate. However, an actor would not meet this condition in the event that it misled an individual about the nature of the consent to be provided, dissuaded individuals from providing consent in respect of disclosures to the actor's competitors, or imposed onerous requirements to effectuate consent that were unnecessary and not required by law.

We seek comment on whether the proposed condition requiring the provision of a meaningful opportunity and prohibiting improper encouragement or inducement should apply to preconditions beyond the precondition that an individual provide consent or authorization. We seek comment on whether the conditions specified for this sub-exception, when taken in total, are sufficiently particularized and sufficiently strict to ensure that actors that are in a position to influence whether a precondition is satisfied will not be able to take advantage of this sub-exception and seek protection for practices that do not promote the privacy of EHI. We also seek comment on whether we should adopt a more tailored approach to conditioning the availability of this exception. For example, we are considering whether different conditions should apply depending on: (i) The nature of the EHI at issue; (ii) the circumstances in which the EHI is being access, exchanged, or used; (iii) the interest being protected by the precondition; or (iv) the nature of the precondition to be satisfied. Commenters are encouraged to identify scenarios in which the application of the conditions applicable to this sub-exception, as proposed, give rise to unnecessary burden, or would require activities that do not advance the dual policy interests of preventing information blocking and promoting privacy and security.

Practice Must Be Tailored to the Specific Privacy Risk or Interest Being Addressed

To qualify for this sub-exception, an actor's privacy-protective practice must be tailored to the specific privacy risks that the practice actually addresses. This condition necessarily presupposes that an actor has carefully evaluated the privacy requirements imposed on the actor, the privacy interests to be managed by the actor, and has developed a considered response that is tailored to protecting and promoting the privacy of EHI. For example, the HIPAA Privacy Rule at 45 CFR 164.514(h) requires that, in certain circumstances, the disclosure of PHI is only authorized once the identity and authority of the person requesting the information has been verified. The privacy issue to be addressed in this instance is the risk that PHI will be disclosed to the wrong individual, or an unauthorized person. If an actor chooses not to provide access, exchange, or use of EHI on the basis that the actor's identity verification requirements have not been satisfied, the actor's practice must be tailored to the specific privacy risks at issue. This would require that the actor ensure that it does not impose identity verification requirements that are unreasonably onerous under the circumstances.

To illustrate, a policy where a driver's license was the only accepted government-issued form of identification would not be a practice that is tailored to the privacy risk at issue because the provider's preference for one form of government-issued identification over another does not meaningfully manage the privacy risk. Similarly, it may be unreasonable for an actor to require the production of documentation demonstrating the parent-child relationship unless the actor was in possession of information that suggested that an adult might not have authority to be the child's legal representative. To do otherwise would be to apply an onerous requirement in all instances of parent-child relationships, which is insufficiently tailored to the privacy risk being managed. Finally, it may be unreasonable for an actor to insist that the individual produce original identification if the individual was able to furnish a scanned copy of their form of identification that the actor could reasonably rely on.

For the purposes of this sub-exception, we clarify that engaging in an interference on the basis that a precondition has not been satisfied would be a practice that addresses a privacy risk or interest, and so tailoring that interference to satisfy a precondition can satisfy this condition. Controls on access, exchange, or use arising under privacy laws serve a privacy interest and so this condition will be met so long as the actor's practice is tailored to the risk or interest being addressed.

We seek comment on this proposed condition.

Practice Must Be Implemented in a Consistent and Non-Discriminatory Manner

We propose that in order for a practice to qualify for this sub-exception, the practice must be implemented in a consistent and non-discriminatory manner. This condition would provide basic assurance that the purported privacy practice is directly related to a specific privacy risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

This condition requires that the actor's privacy-protective practices must be based on objective criteria that apply uniformly for all substantially similar privacy risks. An actor could not, for example, implement an organizational privacy policy that imposed unreasonably onerous requirements on a certain class of individuals or entities without a legitimate justification for doing so. For example, an actor that offered a patient-facing software application (app) would not be able to benefit from this exception if it refused to exchange EHI with a competitor app on the basis of an individual's failure to meet onerous authorization requirements that applied only to health information exchange with the competitor app and did not apply to, for example, the exchange of EHI with health care providers. This condition provides basic assurance that the purported privacy-protective practice is not being used to interfere with access, exchange, or use of EHI for other purposes to which this proposed exception does not apply.

We request comment on this proposed condition.

Sub-Exception to Proposed Privacy Exception: Health IT Developer of Certified Health IT Not Covered by HIPAA

The sub-exception proposed in § 171.202(b) recognizes as reasonable and necessary the activities engaged in by actors consistent with the controls placed on access, exchange, or use of EHI by federal and state privacy laws. Importantly, that sub-exception is limited to actors that are subject to those federal and state privacy laws; an actor that is not regulated by HIPAA or a state privacy law cannot benefit from the exception proposed in § 171.202(b).

We propose to establish a sub-exception to the information blocking provision that would apply to actors that are health IT developers of certified health IT but not regulated by the HIPAA Privacy Rule in respect to the operation of the actor's health IT product or service (referred to hereafter as ''non-covered actors''). We expect that the class of actors to which this proposed sub-exception applies will be very small. The vast majority of health IT developers of certified health IT operate as business associates to health care providers or health plans, are regulated by the HIPAA Privacy Rule, and will be able to benefit from the exception proposed in § 171.202(b) to the extent that the HIPAA Privacy Rule (or applicable state privacy law) imposes preconditions to the provision of access, exchange, or use of EHI. However, we recognize that direct-to-consumer health IT products and services are a growing sector of the health IT market. This class of health IT is often not regulated by the HIPAA Privacy Rule, but could be certified under the Program. We note that the privacy practices of consumer-facing health IT products and services are typically regulated by the Federal Trade Commission Act (FTC Act). However, the FTC Act applies to acts and practices that are unfair and deceptive (15 U.S.C. 45(a)(1)), and does not prescribe privacy requirements to be adopted or followed that can be leveraged for the purpose of recognizing reasonable and necessary privacy-protective practices in this proposed rule.[118]

As discussed in section VIII.C.2.b, where a health IT developer of certified health IT offers a health IT product or service not regulated by the HIPAA Privacy Rule, such product or service is subject to the information blocking provision. We want to ensure that non-covered actors that engage in reasonable and necessary privacy-protective practices that interfere with the access, exchange, or use of EHI can seek coverage under this proposed sub-exception. As such, we propose that a non-covered actor will not engage in information blocking if the actor does not provide access, exchange, or use of EHI where the practice implements a process that is described in the actor's organizational privacy policy and has been disclosed to any individual or entity that uses the actor's health IT. This proposed sub-exception is proposed in § 171.202(c).

As a threshold requirement of this sub-exception, the actor's practice of interfering with access, exchange, or use of EHI must comply with any applicable state or federal privacy laws. While we have developed this sub-exception for the express purpose of addressing privacy-protective practices that are not regulated by the HIPAA Privacy Rule, we acknowledge that there may be other privacy laws implicated by the practice in question. If the actor's practice contravenes a state or federal privacy law, but otherwise satisfies this proposed sub-exception, the actor would not be entitled to benefit from this sub-exception.

Practice Must Implement Privacy Policy

In order to qualify for this sub-exception, the practice engaged in by the non-covered actor—the interference with access, exchange, or use of EHI—must also implement a process described in the actor's organizational privacy policy. This requires that a non-covered actor must have documented in detail in its organizational privacy policy the processes and procedures that the actor will use to determine when the actor will not provide access, exchange, or use of EHI. For example, a non-covered actor that proposed to require the provision of written consent for the use or disclosure of EHI would need to describe in its organizational privacy policy the processes and procedures to be utilized by the actor to implement that privacy-protective practice in order that the practice be considered reasonable and necessary and qualify for this sub- exception. A privacy policy that was prepared at a high level—for example, that simply stated that written consent was required—would not qualify. To build on this example, a non-covered actor's consent policy would need to describe the specific requirements that are imposed on individuals when giving consent, together with the processes and procedures to be followed by the non-covered actor to ensure that the individual has a meaningful choice over whether to consent. Compliance with this condition ensures that this sub-exception recognizes only legitimate practices that have been tailored to the privacy needs of the individuals that use the non-covered actor's health IT, and does not recognize practices that are a pretext or after-the-fact rationalization for actions that interfere with access, exchange, or use of EHI.

It necessarily follows that the non-covered actor's practice must implement its documented organizational privacy policy. For example, if a non-covered actor chose not to provide access, exchange, or use of EHI on the basis that it could not verify the identity of the individual requesting the EHI, the non-covered actor would need to be able to demonstrate that it implemented the

[118] *See* HHS, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA, https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.*

part of its organizational privacy policy that dealt with identity verification. Practices that diverge from an actor's documented policies or practices, or which are not addressed in an actor's organizational privacy policy, would not qualify for this proposed sub-exception.

Practice Must Have Been Disclosed to Users

A non-covered actor that seeks to benefit from this proposed sub-exception must also ensure that it has previously disclosed the privacy-protective practice to the individuals and entities that use, or will use, the health IT. These users are affected by the practices engaged in by a non-covered actor but may otherwise have no visibility of the non-covered actor's approach to protecting the privacy of EHI. We expect that non-covered actors will seek to satisfy this condition by using a privacy notice.[119] We emphasize that the disclosure must be meaningful. In assessing whether a non-covered actor's disclosure was meaningful, regard will be paid to whether the disclosure was in plain language and conspicuous, including whether the disclosure was located in a place, and presented in a manner, that is accessible and obvious to the individuals and entities that use, or will use, the health IT.

To qualify for this sub-exception, a non-covered actor would not be required to disclose its organizational privacy policy to its customers or to the public generally. Rather, the non-covered actor need only describe, with sufficient detail and precision to be readily understood by users of the non-covered actor's health IT, the privacy-protective practices that the non-covered actor has adopted and will observe. This is necessary because a non-covered actor that is not subject to prescribed privacy standards in connection with the provision of health IT will have significant flexibility in the privacy-protective practices that it adopts. If an actor is not required to inform the individuals and entities that use, or will use, the health IT, about the privacy- protective practices that it will implement in its product, or when providing its service, there is a risk that this proposed sub-exception will give deference to policies and processes that are post hoc rationalizations used to justify improper practices. This condition also serves as a check on the nature of the interferences that a non-covered actor writes into its organizational privacy policies; transparency will help to ensure that a non-covered actor takes a balanced approach to protecting privacy interests on one hand, and pursuing business interests that might be inconsistent with the information blocking provision, on the other hand. We hope that this requirement will foster a quasi-market based measure of when a privacy-protective practice is ''reasonable and necessary,'' and ensure that any departure made by a non-covered actor from privacy practices that are recognized by state or federal law is transparent and open.

It will be a matter for non-covered actors to determine the most appropriate way to communicate its privacy practices to users. We believe that it would be reasonable that non- covered actors would, at minimum, post their privacy notices, or otherwise describe their privacy-protective practices, on their websites.

Practice Must Be Tailored to Privacy Risk and Implemented in a Non-Discriminatory Manner

Finally, we propose that in order for a practice to qualify for this sub-exception, an actor's practice must be tailored to the specific privacy risks that the practice actually addresses, and must be implemented in a consistent and non-discriminatory manner. These conditions also apply to the exception proposed in § 171.202(b), and the discussion above addressing these conditions in connection with § 171.202(b) applies to this proposed exception in § 171.202(c). We refer readers to the above discussion and invite comments on these proposed conditions.

We seek comment on this proposed sub-exception generally. Specifically, we seek comment on whether HIEs or HINs would benefit from a similar sub-exception. We also seek comment on whether the conditions applicable to this sub-exception are sufficient to ensure that non-covered actors cannot take advantage of this exception by engaging in practices that are inconsistent with the promotion of individual privacy. We also seek comment on the level of detail that non-covered actors should be required to use when describing their privacy practices and processes to user of health IT.

Sub-Exception to Proposed Privacy Exception: Denial of an Individual's Request for Their Electronic Protected Health Information in the Circumstances Provided in 45 CFR 164.524(a)(1), (2), and (3)

We propose a limited sub-exception to the information blocking provision that would permit a covered entity or business associate to deny an individual's request for access to their PHI in the circumstances provided under 45 CFR 164.524(a)(1), (2), and (3). We believe this exception would avoid a potential conflict between the HIPAA Privacy Rule and the information blocking provision. Specifically, the HIPAA Privacy Rule contemplates circumstances under which covered entities, and in some instances business associates, may deny an individual access to PHI and distinguishes those grounds for denial which are reviewable from those which are not. This exception applies to both the ''unreviewable grounds'' and ''reviewable grounds'' of access. The ''unreviewable grounds'' for denial for individuals include situations involving: (1) Certain requests that are made by inmates of correctional institutions; (2) information created or obtained during research that includes treatment, if certain conditions are met; (3) denials permitted by the Privacy Act; and (4) information obtained from non-health care providers pursuant to promises of confidentiality. In addition, two categories of information are expressly excluded from the individual right of access: (1) Psychotherapy notes, which are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session that are maintained separate from the rest of the patient's medical record (*see* 45 CFR 164.524(a)(1)); and (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding (*see* 45 CFR 164.501).

The ''reviewable grounds'' of access as described in § 164.524(a)(3), which provides that a covered entity may deny access provided that the individual is given a right to have such denials reviewed under certain circumstances. One such circumstance is when a licensed health care professional, in the exercise of professional judgment, determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. In addition, if access is denied, then the individual has the right to have the denial reviewed by a

[119] ONC has provided a Model Privacy Notice (MPN) that is a voluntary, openly available resource designed to help developers clearly convey information about their privacy and security policies to their users. Similar to the FDA Nutrition Facts Label, the MPN provides a snapshot of a company's existing privacy practices encouraging transparency and helping consumers make informed choices when selecting products. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies. See *https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn.*

licensed health professional who is to act as a reviewing official and did not participate in the original decision to deny access (*see generally* 45 CFR 164.524(a)(3)).

We propose that if an actor who is a covered entity or business associate denies an individual's request for access to their PHI on the basis of these unreviewable and reviewable grounds, and provided the denial of access complies with the requirements of the HIPAA Privacy Rule in each case, then the actor would qualify for this exception and these practices would not constitute information blocking.

The following example illustrates this proposed sub-exception. An individual is a patient of a psychiatrist who is a HIPAA covered entity. The patient has requested all of his electronic health files from the psychiatrist. The psychiatrist maintains separately from the electronic health record a file containing psychotherapy notes regarding the patient. The psychiatrist grants access to the patient by providing a copy of the information in his electronic health record, but does not provide the patient's psychotherapy notes. Under this example, the psychiatrist would meet the requirements of this proposed exception since the HIPAA Privacy Rule provides that covered entities can deny individuals access to their psychotherapy notes and provides that this is an unreviewable grounds for denial.

We seek comment on this proposed sub-exception.

Sub-Exception to Proposed Privacy Exception: Respecting an Individual's Request Not To Share Information

We propose to establish an exception to the information blocking provision that would, in certain circumstances, permit an actor not to provide access, exchange, or use of EHI if an individual has specifically requested that the actor not do so. This sub-exception is proposed in § 171.202(e). We believe this sub-exception is necessary to ensure that actors are confident that they can respect individuals' privacy choices without engaging in information blocking, and to promote public confidence in the health IT infrastructure by effectuating patients' preference about how and under what circumstances their EHI will be accessed, exchanged, and used. We recognize that individuals may have concerns about permitting their EHI to be accessed, exchanged, or used electronically under certain circumstances. As a matter of public policy, we think that these privacy concerns, if expressed by an individual and agreed to by an actor, would be reasonable and necessary, and an actor's conduct in abiding by its agreement would, if all conditions are met, be an exception to the information blocking provision.

This proposed sub-exception would not apply under circumstances where an actor interferes with a use or disclosure of EHI that is required by law, including when EHI is required by the Secretary to enforce HIPAA under 45 CFR 164.502(a)(2)(ii) and 45 CFR 164.502(a)(4)(i). Stated differently, this sub-exception would not operate to permit an actor to refuse to provide access, exchange, or use of EHI when that access, exchange, or use is required by law. This sub-exception recognizes and supports the public policy objective of the HIPAA Privacy Rule, which identifies uses and disclosures of EHI for which the public interest in the disclosure of the individual's information outweighs the individual's interests in controlling the information.

This sub-exception would permit an actor not to share EHI if the following conditions are met: (1) The individual made the request to the actor not to have his or her EHI accessed, exchanged, or used; (2) the individual's request was initiated by the individual without any improper encouragement or inducement by the actor; and (3) the actor or its agent documents the request within a reasonable time period.

To qualify for this sub-exception, the request that the individual's EHI not be accessed, exchanged, or used must come from the individual. Moreover, the individual must have made the request independently and without any improper encouragement or inducement by the actor. For example, it would be improper to encourage individuals not to share information with unaffiliated providers on the basis of generalized or speculative risks of unauthorized disclosure. On the other hand, if the actor was aware of a specific privacy or security risk, it would not be improper to inform individuals of that risk. Likewise, an actor would be permitted to provide an individual with general information about her privacy rights and options, including for example, the option to not provide consent, provided the information is presented accurately, does not omit important information, and is not presented in a way that is likely to improperly influence the individual's decision about how to exercise their rights.

If an individual submits a request to an actor not to disclose her EHI, and the actor agrees with and documents the request, the request would be valid for purposes of this sub-exception unless and until it is subsequently revoked by the individual. We believe this approach would minimize compliance burdens for actors while also respecting individuals' requests. We propose that once the individual makes the request, she should not, subject to the requirements of applicable federal or state laws and regulations, have to continually reiterate her privacy preferences, such as having to re-submit a request every year. Likewise, we propose that once the actor has documented an individual's request, the actor should not have to repeatedly reconfirm and re-document the request. We seek comment, however, regarding whether this approach is too permissive and could result in unintended consequences. We also seek comment on this proposed sub-exception generally, including on effective ways for an individual to revoke his or her privacy request for purposes of this sub-exception.

We also propose that in order for a practice to qualify for this sub-exception, an actor's practice must be implemented in a consistent and non-discriminatory manner. This condition would provide basic assurance that the purported privacy practice is directly related to the risk of disclosing EHI contrary to the wishes of an individual, and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply. This condition requires that the actor's privacy-protective practice must be based on objective criteria that apply uniformly for all substantially similar privacy risks.

We note that under the HIPAA Privacy Rule, individuals have the right to request restrictions on how a covered entity will use (as that term is defined in 45 CFR160.103) and disclose PHI about them for treatment, payment, and health care operations pursuant to 45 CFR 164.522(a)(1). Under § 164.522(a), a covered entity is not required to agree to an individual's request for a restriction (other than in the case of a disclosure to a health plan under § 164.522(a)(1)(vi)), but is bound by any restrictions to which it agrees.

We wish to clarify that, for the purposes of this proposed sub-exception, the actor may give effect to an individual's request not to have an actor disclose EHI even if state or federal laws would allow the actor not to follow the individual's request. This is consistent with our position that, absent improper encouragement or inducement, and subject to appropriate conditions, it should not be considered information blocking to give effect to patients' individual preferences about how their EHI will be shared or not. As an illustration, if an individual requests that her EHI not be accessed, exchanged, or used by a physician to help train new staff at a hospital, the physician may agree not to use the individual's EHI for this purpose despite the fact it would not be required by law to agree to such a restriction. Provided the physician has not encouraged or induced the individual to make this request, this sub-exception would apply to the physician's refusal to disclose the information to staff for training purposes.

We seek comments on this sub-exception generally. Specifically, we seek comment on what would be considered a reasonable time frame for documentation. In addition, we also seek comment on how this sub-exception would affect public health disclosures and health care research, if an actor did not share a patient's EHI due to a privacy preference, including any effects on preventing or controlling diseases, injury, or disability, and the reporting of disease, injury, and vital events such as births or deaths, and the conduct of public health surveillance and health care research.

3. Promoting the Security of EHI

We propose to establish an exception to the information blocking provision that would permit actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain conditions. Without this exception, actors may be reluctant to implement security measures or engage in other activities that are reasonable and necessary for safeguarding the confidentiality, integrity, and availability of EHI. This could undermine the ultimate goals of the information blocking provision by discouraging best practice security protocols and diminishing the reliability of the health IT ecosystem.

Robust security protections are critical to promoting patients' and other stakeholders' trust and confidence that EHI will be collected, used, and shared in a manner that protects individuals' privacy and complies with applicable legal requirements. Public confidence in the security of their EHI has been challenged, however, by the growing incidence of cyber-attacks in the health care sector. More than ever, health care providers, health IT developers, HIEs and HINs must be vigilant to mitigate security risks and implement appropriate safeguards to secure the EHI they collect, maintain, access, use, and exchange.

The Cures Act directs the National Coordinator, in consultation with the HHS Office for Civil Rights (OCR), to issue guidance on common ''security barriers'' that prevent the trusted exchange of EHI (section 3022(c)(2) of the PHSA). However, the Cures Act also seeks to promote the security of EHI, which it defines as an element of interoperability (section 3000(9)(A) of the PHSA) and a target area for the policy development to be undertaken by the Health Information Technology Advisory Committee (section 3002(b)(2)(B)(ii) of the PHSA). The inclusion of these provisions promote broader access, exchange, and use of EHI while at the same time continuing to promote the confidentiality, integrity, and availability of EHI through security practices that are appropriate and tailored to identified vulnerabilities and risks.

To qualify for this exception, we propose that an actor's conduct must satisfy threshold conditions. As discussed in detail below, the particular security-related practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI, implemented consistently and in a non-discriminatory manner, and tailored to identified security risks.

While the importance of security practices cannot be overstated, this proposed exception would not apply to *all* practices that purport to secure EHI. Rather, this exception will only be available when the actor's security-based practice satisfies the conditions applicable to this exception. We do not believe it would be appropriate to prescribe a ''maximum'' level of security or to dictate a one-size-fits-all approach for all actors that may not be appropriate in all circumstances and may not accommodate new threats, countermeasures, and best practices in a rapidly changing security landscape. Indeed, security infrastructure varies from organization to organization, and there exist diverse approaches and technology solutions to managing security risks. We do not intend for this proposed exception to dictate a specific security approach when an actor's security posture must be agile and its practices iterative. Moreover, effective security best practices focus on the mitigation and remediation of risks to a reasonable and acceptable level, and not the elimination of all vulnerabilities, so organizations should have the flexibility to assess what vulnerabilities to address and how best to address them while ensuring the confidentiality, integrity, and availability of EHI.

As such, we propose that actors would be able to satisfy this exception through practices that implement either security policies and practices developed by the actor, or case-by-case determinations made by the actor. Whether a security-motivated practice meets this exception would be determined on a case-by-case basis using a fact-based analysis of the conditions set forth below. This approach offers the most appropriate framework for analyzing security practices, which are necessarily driven by and must be tailored to actors' individual circumstances.

We wish to emphasize that the security-based practices implemented by a single physician office with limited technology resources, for example, will be different to those implemented by a large health system, and that this difference does not affect an actor's ability to qualify for this exception. The fact-based approach we propose will allow each actor to implement policies, procedures, and technologies that are appropriate for its particular size, organizational structure, and risks to individuals' EHI.

A fact-based analysis also aligns with the HIPAA Security Rule[120] concerning the security of ePHI. The HIPAA Security Rule does not dictate the security measures that a covered entity or business associate must implement, but instead requires the entity to develop security practices and implement administrative, physical, and technical safeguards that take into account the entity's size, complexity, and capabilities; technical, hardware, and software infrastructure; the costs of security measures; and the likelihood and possible impact of potential risks to ePHI. Under the HIPAA Security Rule, covered entities and business associates are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate. Once covered entities and business associates have completed the risk assessment, they must take security measures sufficient to reduce identified risks and vulnerabilities to reasonable and appropriate levels (45 CFR 164.308(a)(1)(ii)). We note, however, that while our approach is consistent with the regulation of security practices under the HIPAA Security Rule, the fact that a practice complies with the HIPAA Security Rule does not establish that it

[120] The HIPAA Security Rule is located at 45 CFR part 160 and Subparts A and C of Part 164 and 68 FR 8333.

meets the conditions of this proposed exception to the information blocking provision. The HIPAA Security Rule and this proposed exception have different focuses. The HIPAA Security Rule establishes a baseline by requiring certain entities to ensure the confidentiality, integrity, and availability of ePHI by implementing security measures, among other safeguards, that the entities determine are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. In contrast, the purpose of this exception to the information blocking provision is to provide flexibility for reasonable and necessary security practices while screening out practices that purport to promote the security of EHI but that are unreasonably broad, onerous on those seeking access to the EHI, are not applied consistently across/within an organization, or otherwise may unreasonably interfere with access, exchange, or use of EHI.

We propose the following conditions that must be met for an activity or practice to qualify for this exception.

The Practice Must Be Directly Related To Safeguarding the Confidentiality, Integrity, and Availability of EHI

As a threshold condition, the proposed exception would not apply to any practices that are not directly related to safeguarding the security of EHI. In assessing the practice, we would consider whether and to what extent the practice directly addressed specific security risks or concerns. We would also consider whether the practice served any other purposes and, if so, whether those purposes were merely incidental to the overriding security purpose or provided an objectively distinct, non-security-related rationale for engaging in the practice.

We note that it should not be particularly difficult or onerous for an actor to demonstrate, as contemplated above, that its practice was directly related to a specific security risk or concern. For example, the actor may show that the practice was a direct response to a known security incident or threat; or that the practice directly related to the need to verify a person's identity before granting access to EHI; or that the practice was directly related to ensuring the integrity of EHI.

The salient issue under this condition, therefore, would be whether the security practice was actually necessary and directly related to safeguarding EHI. To that end, we would consider the actor's purported basis for adopting the particular security practice, which could be evidenced by the actor's organizational security policy, risk assessments, and other relevant documentation, which most actors are already required to develop pursuant to requirements under the HIPAA Rules.[121] However, we propose that the documentation of an actor's decision-making would not necessarily be dispositive. For example, if the practice had the practical effect of disadvantaging competitors or steering referrals, this could be evidence that the practice was not directly related to the safeguarding the confidentiality, integrity, and availability of EHI. We propose that such an inference would also not be warranted where the actor has not met the other conditions of this exception proposed below, as where the actor's policies were not developed or implemented in a reasonable manner; its security policies or practices were not tailored to specific risks; or it applied its security policies or practices in an inconsistent or discriminatory manner.

The Practice Must Be Tailored to the Specific Security Risk Being Addressed

To qualify for this exception, we propose that an actor's security-related practice must be tailored to specific security risks that the practice actually addressed. This condition necessarily presupposes that an actor has carefully evaluated the risk posed by the security threat and developed a considered response that is tailored to mitigating the vulnerabilities of the actor's health IT or other related systems. For example, the awareness of a security vulnerability in a particular HIE's technology may justify a health care provider's suspending access to EHI from that organization or by participants of that HIE, but only for the period in which the threat persists. In contrast, a response that suspended access by all HIEs or that persisted even after the HIE had addressed the security vulnerability in its technology would not be tailored to address specific risks and would not meet this condition.

As another example, it may be reasonable for a health care provider to refuse to grant access to EHI when an individual has been unable to prove her identity. However, the actor's identity proofing practice would have to be tailored to address risks specifically associated with the disclosure of EHI to unauthorized individuals. For example, identity proofing requirements might be tailored if the practice is based on a risk assessment and best practice policies and procedures and is applied consistently and in a non-discriminatory manner. However, we believe an identity proofing requirement would not be tailored if it were not based on an objectively reasonable security risk assessment and a careful consideration of alternative approaches that could adequately address the specific risk of patient misidentification in a less restrictive fashion.

As a final example, an actor's decision to deny access to the EHI it maintains may be reasonable if the practice responds to a request for EHI from a patient-facing website or application that causes the actor's system to raise a malicious software detection alert or if the request comes from a website or application listed on a security ''blacklist.'' However, we propose that the actor's response must be tailored to the specific threat. Among other things, the denial of access must be limited to the patient and/or their personal software. So as to ensure that the response is properly tailored, it would be best practice for actors to ensure that they communicate to those persons whose access was denied the reason for the denial of access, and communicate objective timeframes (if feasible to do so) and other parameters for when access would be granted or restored. Moreover, we propose that, to the extent that the practice implements an organizational security policy, the policy must align with applicable consensus-based standards or best practices for responding to these types of incidents. Disagreement with the individual about the worthiness of the third party as a recipient of EHI, or even concerns about what the third party might do with the EHI, except for reasons such as those listed in the ''preventing harm'' exception, are not acceptable reasons to deny an individual's request.

Practice Must Be Implemented in a Consistent and Non-Discriminatory Manner

We propose that in order for a practice to qualify for this proposed exception, the actor's practice must have been implemented in a consistent and non-discriminatory manner. This condition would provide basic assurance that the purported security practice is directly related to a specific security risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

As an illustration solely of the non-discriminatory manner condition, consider a health IT developer of certified health IT that offers apps to its customers via an app marketplace. If the

[121] 45 CFR 164.306(d)(3)(ii)(B)(1); 45 CFR 164.316(b)(1).

developer requires that third-party apps sold (or made available) via the developer's app marketplace meet certain security requirements, those security requirements must be imposed in a non-discriminatory manner. This would mean, for example, that if a developer imposed a requirement that third-party apps include two-factor authentication for patient access, the developer would need to ensure that the same requirement was imposed on, and met by, all other apps, including any apps made available by the developer itself. To note, such a developer requirement must also meet the other conditions of this exception (*e.g.,* the condition that the practice be tailored to the specific security risk being addressed).

Practices That Implement an Organizational Security Policy

As discussed above, an actor's approach to information security management will reflect the actor's particular size, organizational structure, and risk posture. Because of this, it is important that actors develop and implement organizational policies that secure EHI. We propose that, where an actor has documented security policies that align with applicable consensus-based standards, and where the policies are implemented in a consistent and non-discriminatory manner, a practice's conformity with such policies would provide a degree of assurance that the practice was reasonable and necessary to address specific security risks and thus should not constitute information blocking. Conversely, a practice that went beyond an actor's established policies or practices by imposing security controls that were not documented, would not qualify for this exception under this condition (although the actor may be able to qualify under the alternative basis for practices that do not implement a security policy). Further, such practices would be suspect under the information blocking provision if there were indications that the actor's security-related justifications were a pretext or after-the-fact rationalizations for its actions or was otherwise unreasonable under the circumstances.

We reiterate that, to the extent that an actor seeks to justify a practice on the basis of its organizational security policies, such policies must be in writing and implemented in a consistent and non-discriminatory manner. As noted above, what a policy requires will depend on the facts and circumstances. However, we propose that to support a presumption that a practice conducted pursuant to the actor's security policy was reasonable, the policy would have to meet the following conditions.

- *Risks identified and assessed.* The actor's security policy must be informed by an assessment of the security risks facing the actor. While we do not propose any requirements as to a risk assessment, we note that a good risk assessment would use an approach consistent with industry standards,[122] and would incorporate elements such as threat and vulnerability analysis, data collection, security measures, likelihood of occurrence, impact, level of risk, and final reporting.[123]
- *Consensus-based standards or best practice guidance.* The actor's policy must align with one or more applicable consensus-based standards or best practice guidance. At present, examples of relevant best practices for development of security policies include, but are not limited to: NIST–800–53 Rev. 5; the NIST Cybersecurity Framework; and NIST SP 800–100, SP 800–37 Rev. 2, SP 800–39, as updated and as interpreted through formal guidance. Best practice guidance on security policies is also developed by consensus standards bodies such as ISO, IETF, or IEC. HIPAA covered entities and business associates may be able to leverage their HIPAA Security Rule compliance activities and can, if they choose, align their security policy with those parts of the NIST Cybersecurity Framework that are referenced in the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework to satisfy this condition. Relevant consensus-based standards and frameworks provide actors of varying size and resources with the flexibility needed to apply the right security controls to the right information systems at the right time to adequately address risk.
- *Objective timeframes and other parameters.* We propose that the actor's security policy must provide objective timeframes and common terminology used for identifying, responding to, and addressing security incidents. Examples of acceptable sources for development of a security response plan include: NIST Incident Response Procedure (*https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final*), US–CERT for interactions with government systems (*https://www.us-cert.gov/government-users/reporting-requirements*), and ISC–CERT for critical infrastructure (*https://ics-cert.us-cert.gov/*).

As a point of clarification, we note that an actor's compliance with the HIPAA Security Rule (if applicable to the actor) would be relevant to, but not dispositive of, whether the actor's policies and procedures were objectively reasonable for the purpose of this exception. An actor's documentation of its security policies and procedures for compliance with the Security Rule may not offer a basis to evaluate whether the actor's security practices unnecessarily interfere with access, use, or exchange of EHI. For example, it could be difficult to determine whether a practice unnecessary interferes with exchange of EHI based on a review of the customized PHI data flow diagram the actor prepared as part of its Security Rule risk analysis. We believe that a documented policy that provides explicit references to consensus-based standards and best practice guidance (such as the NIST Cybersecurity Framework) offer an objective and robust means for ONC and the OIG to evaluate the reasonableness of a particular security control for the purpose of this exception.

We recognize that, as a practical matter, some actors (such as small health care providers or those with limited resources) may have organizational security policies that are less robust or that otherwise fall short of the minimum conditions proposed above. As discussed immediately below, we propose that in these circumstances an actor could still benefit from this proposed exception by demonstrating that the practice at issue was objectively reasonable under the circumstances, without regard to a formal policy.

Practices That Do Not Implement an Organizational Security Policy

While we expect that most security practices engaged in by an actor will implement an organizational policy, we recognize that EHI security may present novel and unexpected threats that even a best-practice risk assessment and security policy cannot anticipate. If a practice that does not implement an organizational policy is to qualify for this exception, however, it must meet certain conditions. The actor's practice must, based on the particularized facts and circumstances, be necessary to mitigate the security risk. Importantly, we propose that the actor would have to demonstrate that it considered reasonable and appropriate alternatives that could have reduced the likelihood of interference with access, exchange, or use of EHI, and that there were no reasonable and appropriate alternatives

[122] See OCR, Guidance on Risk Analysis, *https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.*

[123] ONC and OCR have jointly launched the HHS HIPAA Security Risk Assessment (SRA) Tool, *https://www.healthit.gov/providers-professionals/security-risk-assessment-tool.*

that were less likely to interfere with access, exchange or use of EHI.

We note that an actor's consideration of reasonable and appropriate alternatives will depend on the urgency and nature of the security threat in question. We anticipate that an actor's qualification for this exception would accommodate exigent circumstances. For example, we would not expect an actor to delay the implementation of a security measure in response to an emergency on the basis that it has not yet been able to initiate a fully realized risk assessment process. However, we expect that in these exigent circumstances, where the actor has implemented a security practice without first considering whether there were reasonable and appropriate alternatives that were less likely to interfere with access, exchange or use of EHI, the actor would expeditiously make any necessary changes to the practice based on the actor's consideration of reasonable and appropriate alternatives that are less likely to interfere with access, exchange or use of EHI. We propose that the exception would apply in these instances so long as an actor takes these steps and complies with all other applicable conditions.

We encourage comment on these conditions and our overall approach to this proposed exception, including whether our proposal provides adequate flexibility for actors to implement measures that are commensurate to the threats they face, the technology infrastructure they possess, and their overall security profiles and, equally important, whether this exception adequately mitigates the risk that actors will adopt security policies that are unnecessarily restrictive or engage in practices that unreasonably interfere with access, exchange, or use of EHI. Commenters are encouraged to propose additional conditions that may be necessary to ensure that the exception is tailored and does not extend protection to practices that are not reasonable and necessary to promote the security of EHI and that could present information blocking concerns. We also seek comment on whether the use of consensus-based standards and guidance provides an appropriate reference point for the development of security policies. Finally, commenters may wish to offer an alternative basis for identifying practices that do not offer a security benefit (compared with available alternatives) but that cause an information blocking harm by interfering with access, exchange, or use of EHI.

4. Recovering Costs Reasonably Incurred

We propose to establish an exception to the information blocking provision that would permit the recovery of certain costs reasonably incurred to provide access, exchange, or use of EHI. The exception and corresponding conditions are set forth in the proposed regulation text in § 171.204. We interpret the definition of information blocking to include *any* fee that is likely to interfere with the access, exchange, or use of EHI (see discussion in section VIII.C.4.c.iv). We anticipate that this interpretation may be broader than necessary to address genuine information blocking concerns and could have unintended consequences on innovation and competition. Specifically, unless we establish an exception, actors may be unable to recover costs that they reasonably incur to develop technologies and provide services that enhance interoperability. This could undermine the ultimate goals of the information blocking provision by diminishing incentives to invest in, develop, and disseminate interoperable technologies and services that enable more robust access, exchange, and use of EHI. Therefore, we propose to establish an exception that would permit the recovery of certain costs that we believe are unlikely to present information blocking concerns and would generally promote innovation, competition, and consumer welfare, provided certain conditions are met. We note that complying with the requirements of this exception would not prevent an actor from making a profit in connection with the provision of access, exchange, or use of EHI. Indeed, the costs recoverable under this proposed exception could include a reasonable profit, provided that all applicable conditions were met.

The exception would be subject to strict conditions to prevent its potential misuse. Specifically, we are concerned that a broad or insufficiently tailored exception for the recovery of costs could protect rent-seeking, opportunistic fees, and exclusionary practices that interfere with the access, exchange, and use of EHI. These practices fall within the definition of information blocking and reflect some of the most serious concerns that motivated its enactment (*see* section VIII.B of this preamble). For example, in the Information Blocking Congressional Report, we cited evidence of wide variation in fees charged for health IT products and services. While we cautioned that the issue of fees is nuanced, and that variations in fees could be attributable in part to different technology architectures, service models, capabilities, service levels, and other factors, we concluded that these factors alone could not adequately explain all of the variation in prices that we had observed. Based on these and other indications, we concluded that some actors were engaging in opportunistic pricing practices or, in some cases, charging prices designed to deter connectivity or exchange with competing technologies or services.

In the time since we published the Information Blocking Congressional Report, these practices have persisted and, in certain respects, become more pronounced. In a national survey of HIE executives published in 2017, 47% of respondents reported that EHR developers ''often/routinely'' charge high fees for exchange that are unrelated to cost, and another 40% reported that they ''sometimes'' do.[124] Meanwhile, we have continued to receive credible evidence of rent-seeking and other opportunistic behaviors, such as fees for data export and data portability that are not plausibly related to any reasonable time, materials, or other costs that a developer would reasonably incur to provide these services. And, while some practices described in the Information Blocking Congressional Report have become less prevalent (such as the charging of per-transaction fees), other practices have emerged that are equally concerning.

As just one illustration, some EHR developers have begun conditioning access or use of customer EHI on revenue-sharing or royalty agreements that bear no plausible relation to the costs incurred by the EHR developer to grant access to the EHI. We have also heard of discriminatory pricing policies that have the obvious purpose and effect of excluding competitors from the use of interoperability elements. Many of the industry stakeholders who shared their perspectives with us in listening sessions prior to this proposed rule, including several health IT developers of certified health IT, condemned these practices and urged us to swiftly address them.

In light of these concerns, we propose that this exception would apply only to the recovery of certain costs and only when the actor's methods for recovering such costs comply with certain conditions at all relevant times. As discussed in more detail below, these conditions would require that the costs the actor recovered were reasonably

[124] Julia Adler-Milstein and Eric Pfeifer, *Information Blocking: Is It Occurring And What Policy Strategies Can Address It?,* 95 Milbank Quarterly 117, 124–25 (Mar. 2017), *available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full.*

incurred and did not reflect costs that are speculative or subjective. Actors would also be required to allocate costs in an appropriate manner and to use objective and permissible criteria when charging fees to recover those costs. Further, the exception would not apply to certain fees, such as those based on the profit or revenue associated with the use of EHI (either being earned by the actor, or that could be realized by another individual or entity) that exceed the actor's reasonable costs for providing access, exchange, or use of the EHI. We specify certain prohibited fees below.

Finally, the exception would provide additional conditions applicable to fees charged in connection with: (1) The certified APIs described in § 170.404; and (2) the EHI export capability proposed in § 170.315(b)(10) for the purposes of switching health IT or to provide patients their electronic health information. We emphasize that access to EHI that is provisioned by supplying some form of physical media, such as paper copies (where the EHI is printed out), or where EHI is copied onto a CD or flash-drive, would not be a practice that implicated the information blocking provision provided that the fee(s) charged for that access complied with HIPAA (45 CFR 164.524(c)(4)).

Our intention with this exception is not to set any particular cost that would be considered ''reasonably incurred,'' but rather to allow the market to define the appropriate price so long as certain methods are followed and certain criteria are met.

Requirement That Costs Be Reasonably Incurred

Regardless of the type of cost at issue, a basic condition of this proposed exception is that any costs the actor seeks to recover must have been reasonably incurred to provide the relevant interoperability elements to enable access, exchange, or use of EHI. Ultimately, whether a cost was reasonably incurred will depend on the particular facts and circumstances. We believe this fact-based approach is appropriate in light of the considerable diversity in the types of costs that actors might incur and the range of factors that could bear on the reasonableness of those costs. For example, the costs of developing software may vary with the purposes it is intended to serve, the settings in which it will be deployed, the types and scope of capabilities included, and the extent to which these development efforts build on existing development efforts and know-how. Additionally, the costs of providing services, including the implementation of technology in production environments, may vary based on the technology design or architecture, individual customer needs, local implementation conditions, and other factors. An analysis of costs would also account for different distribution and service models under which the costs are calculated. We seek comment on these and other considerations that may be relevant to assessing the reasonableness of costs incurred for purposes of this exception.

Method for Recovering Costs

To qualify for the exception, we propose that the method by which the actor seeks to recover its costs must be reasonable and non-discriminatory. This would require that the actor base its recovery of costs on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. We emphasize that this proposal does not mean that the actor must apply the same prices or price terms for all persons or classes of persons to whom it provides the services. However, any differences in prices or price terms would have to be based on actual differences in the costs that the actor incurred or other reasonable and non-discriminatory criteria. We further propose to require that the method by which the actor recovers its costs must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged.

We also propose that the method by which the actor recovers its costs must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported. A reasonable allocation of costs would require that the actor allocate its costs in accordance with criteria that are reasonable and between only those customers that either cause the costs to be incurred or benefit from the associated supply or support of the technology. If an actor developed technology that could be supplied to multiple customers with minimal tailoring, the core costs of developing its technology should be allocated between those customers when recovered as a fee. The actor would not be permitted to recover the total of its core costs from each customer. Similarly, when an actor uses shared facilities and resources to support the usage of technology, it would need to ensure that those shared costs were reasonably allocated between all of the customers that benefited from them. However, whenever an actor is required to provide services and incur costs that are unique to a particular customer, it would not need to distribute those costs among other customers that had deployed technology.

In addition, the exception would not apply if the method by which the actor recovers its costs is based, in any part, on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor. The use of such criteria would be suspect because it suggests the fee the actor is charging is not based on its reasonable costs to provide the services and may have the purpose or effect of excluding or creating impediments for competitors, business rivals, or other persons engaged in developing or enabling the use of interoperable technologies and services.

Last, we propose that the method by which the actor recovers its costs must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that *exceeds* the actor's reasonable costs for providing access, exchange, or use of electronic health information. We emphasize that such revenue-sharing or profit-sharing arrangements would *only* be acceptable and covered by the exception if such arrangements are designed to provide an alternative way to recover the costs reasonably incurred for providing services.

We seek comment on these conditions and other issues we should consider in assessing whether the methodology by which an actor distributes costs and charges fees should be considered reasonable and necessary for purposes of this exception. In particular we are considering whether to introduce specific factors and methods for assessing when profit will be reasonable. For example, should the pro-competitive or efficiency-adding aspect of an actor's approach to providing access, exchange, or use of EHI be taken into account when assessing the reasonableness of the profit recovered by an actor? We also ask commenters to consider whether there are specific use cases for which actors' profits should be limited or prohibited. We request that commenters provide as much detail as possible when describing methods for quantifying profits and evaluating their reasonableness.

Costs Specifically Excluded

We propose that certain costs should be explicitly excluded from this exception regardless of the method for recovering the costs. We have proposed these excluded costs, which are detailed below, in an effort to provide additional clarity about the scope of this exception and to create guardrails for preventing potential misuse of the exception.

Costs Due to Non-Standard Design or Implementation Choices

We propose that this exception would not permit the recovery of any cost that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI. To the extent that such costs can be reasonably avoided, we believe that actors should internalize the costs of such behaviors, which do not benefit consumers, and which create unnecessary impediments to access, exchange, and use of EHI. As an illustration, if a health IT developer of certified health IT designed its database tables or other aspects of its technology in ways that make exporting or converting EHI to other formats difficult, the developer could not claim that its costs to provide data conversion services to customers are reasonably incurred. Such costs would not be eligible under this exception (and might implicate the information blocking provision for the reasons noted in section VIII.C.4.c.v of this preamble).

We welcome comments on the exclusion of these types of costs.

Subjective or Speculative Costs

We propose to limit this exception to the recovery of costs that an actor *actually* incurred to provide the relevant interoperability element or group of elements (which may comprise either products or services). We propose that this exception would not permit the recovery of certain types of costs that are subjective or speculative. We note two important examples of this limitation.

First, an actor would not be permitted to recover any costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets. For example, an actor could not charge a customer a fee based on the purported ''cost'' of allowing the customer to use the actor's patented technology, computer software, databases, trade secrets, copyrighted works, and the like. We understand that the customer's use of the asset could be considered a ''cost'' in the sense that, were it not for the information blocking provision, the actor could charge a royalty or other fee for the use of its intangible assets. For this reason, in section VIII.D.6, we propose to permit an actor to license most interoperability elements on reasonable and non-discriminatory terms, subject to certain conditions. For purposes of this more general exception, however, we believe it would be inappropriate to permit an actor to charge a fee based on these considerations, which are inherently subjective and could invite the kinds of rent-seeking and opportunistic pricing practices that fall squarely within the definition of information blocking. We clarify that an actor's practices could qualify for both this exception (recovering costs reasonably incurred) and the exception for licensing of interoperability elements on reasonable and non-discriminatory terms in section VIII.D.6. In that case, the actor could recover costs under both exceptions.

Second, and for similar reasons, an actor would not be permitted to recover costs that are speculative. The exception would not apply to ''opportunity costs,'' such as the revenues that an actor could have earned had it not provided the interoperability elements. We clarify that the exclusion of opportunity costs would not preclude an actor from recovering its reasonable forward-looking cost of capital. We believe these costs are relatively concrete and that permitting their recovery will protect incentives for actors to invest in developing and providing interoperability elements.

Fee Prohibited by 45 CFR 164.524(c)(4)

We also propose that the exception would not apply to fees prohibited by 45 CFR 164.524(c)(4). The HIPAA Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) Labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (*e.g.,* CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual (45 CFR 164.524(c)(4)). The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by state law.

Individual Electronic Access

We propose that this exception would not apply if the actor charged a fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's EHI. Such fees are distinguished from the cost-based fees that a covered entity is permitted to charge individuals for the provision of copies of ePHI under HIPAA (45 CFR 164.524(c)(4)), and similar allowable costs under state privacy laws, which would *not* be excluded from the costs recoverable under this exception. To be clear, access to EHI that is provisioned by supplying some form of physical media, such as paper copies (where the EHI is printed out), or where EHI is copied onto a CD or flash-drive, would not be a practice that implicated the information blocking provision provided that the fee(s) charged for that access complied with HIPAA (45 CFR 164.524(c)(4)).

A fee based on electronic access by an individual or their personal representative, agent, or designee to the individual's EHI, in contrast, would arise if an actor sought to impose on individuals, or their personal representatives, agents, or designees, a fee that operated as a toll for the provision of electronic access. For example, a health care provider that charges individuals a fee in order that the individuals be given access to their EHI via the health care provider's patient portal or another mode of web-based delivery, would not be able to benefit from this exception. Similarly, where an individual authorizes a consumer-facing app to retrieve EHI on the individual's behalf, it would be impermissible for an actor to charge the app or its developer a fee to access or use APIs that enable access to the individual's EHI. This would be true whether the actor is a supplier of the API technology or an individual or entity that has deployed the API technology, such as a health care provider.

Export and Portability of EHI Maintained in EHR Systems

The definition of information blocking specifically mentions transitions between health IT systems and the export of complete information sets as protected forms of access, exchange, and use (*see* section 3022(a)(2)(C)(i) of the PHSA). In our experience, health care providers frequently encounter rent-seeking and opportunistic pricing practices in these and other contexts in which they are attempting to export EHI from their systems for use in connection with other technologies or services that compete with or could reduce the revenue opportunities associated with an EHR developer's own suite of products and services. As discussed in section VIII.C.5.b.iii of this preamble, most EHI is currently maintained in EHRs and other source systems that use proprietary data models or formats; this puts EHR developers in a unique position to block the export and portability of EHI for use in competing systems or applications, or to charge rents for access to the basic technical information needed to facilitate the conversion or migration of data for these purposes. The concerns are compounded by the fact that EHR developers rarely disclose in advance the fees they will charge for data export and data portability services (*see* 80 FR 62719; 80 FR 16880–81).

For the reasons above, we propose that fees charged for the export, conversion, or migration of data from an EHR technology would not qualify for the exception unless they also meet two additional conditions.

First, we propose that health IT developers of certified health IT would, for purposes of this exception, be precluded from charging a fee to perform an export of EHI via the capability of health IT certified to the proposed 2015 Edition ''EHI export'' certification criterion (§ 170.315(b)(10)) for the purposes of switching health IT systems or to provide patients their EHI. As part of the ''Assurances'' Condition of Certification, health IT developers that produce and electronically manage EHI would need to be certified to the ''EHI export'' criterion and provider the functionality to its customers (*see* § 170.402(a)(4) and section VII.B.2.b of this preamble). As described in section IV.C.1 of this preamble, the ''EHI export'' certification criterion is intended to provide a baseline capability to export EHI from certified health IT in a commercially reasonable format in support of transitioning of EHI between health IT systems and patient access. Fees or limitations associated with the use of this capability (as distinguished from deployment or other costs reasonably incurred by the developer) would not receive protection under the exception and may be suspect under the information blocking provision. We clarify that this condition would not preclude a developer from charging a fee to deploy the EHI export capability in a health care provider's production environment, or to provide additional services in connection with this capability other than those reasonably necessary to enable its intended use. For example, this condition would not preclude a developer from charging a fee to perform an export of EHI via the capability of health IT certified to the proposed § 170.315(b)(10) for a third-party analytics company. We emphasize once again that these excluded fees are distinguished from the cost-based fees that a covered entity is permitted to charge individuals for the provision of copies of ePHI under HIPAA (45 CFR 164.524(c)(4)), and similar allowable costs under state privacy laws, which would *not* be excluded from the costs recoverable under this exception.

We note that, because this certification criterion provides only a baseline capability for exporting data, we anticipate that health IT developers of certified health IT will need to provide other data portability services to facilitate the smooth transition of health care providers between different health IT systems. We propose that such fees may qualify for protection under the exception, but only if they meet the other conditions described above and in proposed § 171.205(a).

Second, we propose that the exception would not apply to a fee to export or convert data from an EHR technology unless such fee was agreed to in writing at the time the technology was acquired, meaning when the EHR developer and the customer entered into a contract or license agreement for the EHR technology. This condition is designed to promote the disclosure of fees upfront and thereby reduce the potential for actors to engage in installed-base opportunism or attempting to use fees to discourage data portability.

Compliance With the Condition of Certification Specific to API Technology Suppliers and API Data Providers

We note that health IT developers of certified health IT subject to the API Condition of Certification proposed in § 170.404 may not charge certain types of fees and are subject to more specific cost accountability provisions than apply generally under this proposed exception. We believe that the failure of developers to comply with these additional requirements would impose impediments to consumer and other stakeholder access to EHI without special effort and would be suspect under the information blocking provision. We propose, therefore, that a health IT developer of certified health IT subject to the API Condition of Certification must comply with all requirements of that condition for all practices and at all relevant times in order to qualify for this exception.

We also believe that a health care provider that acts as an API Data Provider, should be subject to the same constraints. For example, the API Condition of Certification prohibits a health IT developer from charging a usage fee to patient-oriented apps. We believe information blocking concerns would arise if a provider were to charge such a fee, notwithstanding the fact that the provider is not subject to the certification requirements. For this reason, we propose that, if the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404. In other words, to the extent that a provider is an API Data Provider, the provider will not qualify for this exception if it charges any fee that a health IT developer of certified health IT would be prohibited from charging under the API Condition of Certification.

Application of the Exception to Individual Practices

We clarify that the conditions of this exception, including those governing the methodology and criteria by which an actor calculates and distributes its costs, must be satisfied for *each and every* fee that an actor charges to a customer, requestor, or other person. For example, if an actor uses a cost allocation methodology that does not meet the requirements of the exception, each fee charged on the basis of that methodology would be a suspect practice under the information blocking provision. All applicable conditions of the exception must be met at all relevant times for each practice.

We request comment on this proposed exception. Specifically, we ask commenters to consider alternate approaches to the exception that would also achieve the goal of allowing actors to recover certain types of costs that would promote innovation, competition and consumer welfare and that are unlikely to present information blocking concerns. In assessing other potential approaches to this exception, we encourage commenters to contemplate such considerations as enforceability, potential burden on the parties, and overall effectiveness in meeting the above stated goals.

5. Responding To Requests That are Infeasible

We propose to establish an exception to the information blocking provision that would permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, provided certain conditions are met. The exception and corresponding conditions are set forth in the proposed regulation text in § 171.205. We propose that this exception would not apply when a response is required by law. As discussed in section VIII.C.5 of this preamble, we propose that the information blocking provision would be implicated if an actor were to refuse to facilitate access, exchange, or use of EHI, either as a general practice or in isolated instances. However, we believe that in certain circumstances legitimate practical challenges beyond an actor's control may limit its ability to comply with requests for access, exchange, or use. In some cases, the actor may not have—and may be unable to obtain—the requisite technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, exchange, or use. In other cases, the actor may be able to comply with the request, but only by incurring costs or other burdens that are clearly unreasonable under the circumstances.

Actors confronted with these types of practical challenges may be concerned about their exposure under the information blocking provision, which could lead to inefficient outcomes. For example, health care providers may feel compelled to entertain requests to enable or support means of exchange or use that would be disruptive to health care operations or that are not financially sustainable. In some of these instances, the actor may be able, but reluctant, to offer alternative means that would meet the requestor's needs while reducing the burden on the actor, leading to more efficient outcomes overall. Actors could also be forced into a ''reactive'' posture that limits their ability to make holistic decisions and to implement health IT in a considered, scalable way that facilitates robust interoperability and information sharing. These outcomes would be counterproductive to the policies the information blocking provision encompasses.

The proposed exception would alleviate some of these concerns while safeguarding against pretextual and other unreasonable refusals to provide access, exchange, or use of EHI. The exception would permit an actor to decline a request in certain narrowly-defined circumstances when doing so would be infeasible (or impossible) and when the actor otherwise did all that it reasonably could do under the circumstances to facilitate alternative means of accessing, exchanging, and using the EHI. We believe this approach is principled and tailored in a manner that will promote basic fairness and encourage parties to work cooperatively to implement efficient solutions to interoperability challenges. Importantly, to ensure that the exception is not used inappropriately, we propose a structured, fact-based approach for determining whether a request was in fact ''infeasible'' within the meaning of this exception. This approach would be limited to a consideration of factors specifically delineated in the exception and that focus the infeasibility inquiry on the immediate and direct financial and operational challenges of facilitating access, exchange, and use, as distinguished from more remote, indirect, or speculative types of injuries.

We encourage comment on these and other aspects of this proposal, which are described in more detail below.

i. Infeasibility of Request

To qualify for this proposed exception, in addition to meeting other conditions, we propose that compliance with the request for access, exchange, or use must be infeasible. We propose a two-step test that an actor would need to meet in order to demonstrate that a request was infeasible.

Complying With the Request Would Impose a Substantial Burden on the Actor

Under the first step of the infeasibility test, the actor would need to show that complying with the particular request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances. We anticipate that in most cases an actor would meet this requirement by showing that it did not have, and could not readily obtain, the requisite technological capabilities, legal rights, or other means necessary to facilitate the particular type of access, exchange, or use requested. Additionally, the requirement could be met by showing that, had it complied with the request, the actor would have experienced a significant disruption to its health care or business activities or would have incurred significant unbudgeted costs. We would also consider other analogous outcomes that impact the actor's health care or business activities in a direct and substantial way. We seek comment on what those outcomes might be and encourage commenters to be as detailed and specific as possible.

In determining whether these or other types of burdens are substantial, we would consider the actor's particular circumstances, including the type of actor; the nature and purpose of its business or other activities; and the financial, technical, and other resources and expertise at its disposal. In addition, we would also consider any offsetting benefits to the actor of providing the requested access, exchange, or use, such as facilitating the actor's compliance with statutory and regulatory requirements. Due to the variability of circumstances, ONC would take a fact-specific approach to these analyses.

As an illustration, a small physician practice with limited financial and technical resources may find it burdensome to accommodate requests from other providers to establish and maintain outbound interfaces from the practice's EHR system that it neither needs for its own health care activities nor to comply with any regulatory requirements. In contrast, a large health system with a well-resourced IT department may be in a position to accommodate such requests without significant disruption to its business and at relatively minimal additional expense relative to its overall IT budget. Similarly, custom development or other activities that might be burdensome for a health care provider with limited technical expertise may not result in a substantial burden for a health IT developer, exchange, or network whose business is to develop and provide technological solutions.

We clarify that the exception focuses solely on the immediate and direct financial and operational challenges of facilitating access, exchange, or use. The exception does not apply—and we would give no weight—to any putative burdens that an actor experiences that relate primarily to the actor's pursuit of an economic advantage, such as its ability to charge higher prices, capture additional revenue streams, maintain or increase its market share, or otherwise pursue its own economic interests. To the extent that these interests merit an exception under the information blocking provision, they are addressed under the exceptions proposed in §§ 171.204 and 171.206. In the same way, the exception would not apply to any putative burdens that are more appropriately examined under another proposed exception. For example, an actor could not claim that it is burdensome to implement a tailored organizational patient safety policy under proposed § 171.201(b) or to develop and implement policies and procedures for satisfying preconditions imposed by state or federal privacy laws for the provision of access, exchange, or use of EHI under proposed § 171.202(b).

The Burden Imposed on the Actor Would Be Plainly Unreasonable Under the Circumstances

To show that a request for access, exchange, or use was infeasible, the actor must not only demonstrate that complying with the request would have resulted in a substantial burden, as described above; the actor must also demonstrate that requiring it to comply with the request—and thus to assume the substantial burden demonstrated under the first part of the test—would have been plainly unreasonable under the circumstances. Whether it would have been plainly unreasonable for the actor to assume the burden of providing access, exchange, or use will be highly dependent on the particular facts and circumstances. While for this reason we do not believe that bright-line rules would be appropriate, we do propose to rely primarily on the following key factors enumerated in proposed § 171.205(a)(1):

- The type of EHI and the purposes for which it may be needed;
- The cost to the actor of complying with the request in the manner requested;
- The financial, technical, and other resources available to the actor;
- Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged;
- Whether the actor maintains ePHI on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains EHI on behalf of the requestor or another person whose access, exchange, or use of EHI will be enabled or facilitated by the actor's compliance with the request;
- Whether the requestor and other relevant persons can reasonably access, exchange, or use the information from other sources or through other means; and
- The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

As these factors suggest, the starting point for our inquiry would be to identify the type of EHI at issue and the purposes for which it may be needed. As explained in section VIII.C.5.b.i. of this preamble, certain types of EHI—namely, observational health information—give rise to a heightened risk of interference under the information blocking provision. For purposes of this exception and the information blocking provision more generally, the actor has a strong duty to facilitate the availability and use of this information, which may be needed for important activities for which timely and complete access to EHI is essential, such as providing patients with their EHI; enabling the use of EHI for treatment and care coordination; and making EHI available for quality improvement and population health management activities.

Next, we would consider the severity of the burdens that the actor would have experienced to provide the access, exchange, or use of EHI in the manner requested. For this purpose, we would consider both the burden on the actor of complying with the specific request at issue as well as the burden the actor would experience if it was required to comply with similar types of requests. We would also consider the observed or likely frequency of such requests. As already discussed, we anticipate that the extent of any burden would depend in part on the particular circumstances of the actor. In addition, in considering the burden to the actor, we would also consider any offsetting benefits to the actor of providing the requested access, exchange, or use.

Having ascertained the nature and severity of any burdens that the actor would assume to provide the requested access, exchange, or use, we would balance these burdens against the countervailing costs to the requestor and other persons (including consumers) who would be harmed by the actor's refusal to provide the requested access, exchange, or use. Importantly, we would consider whether the requestor and other persons could have obtained the EHI from other sources or through other means, including those made available by the actor as an accommodation to the requestor, as discussed in more detail below. If alternative means were available, we would examine the extent to which they would have been appropriate for the purposes for which the EHI or interoperability elements were needed and the extent to which requiring the requestor to pursue these alternative means would impose additional costs or burdens on the requestor and other persons. For example, if the EHI was readily available through other means that were equally efficacious, the actor's refusal to provide yet one more means of access, exchange, or use might impose only a minimal burden on the requestor and other persons' use of the EHI. In contrast, if the actor conditions critical technology or infrastructure for accessing, exchanging, or using EHI, or if its control over other interoperability elements means that EHI cannot be efficiently accessed, exchanged, or used without the actor's cooperation, requiring the requestor to pursue other means of access, exchange, or use would likely be unrealistic and represent an insurmountable burden.

One final consideration would inform our analysis. We would consider the balancing of relative burdens in conjunction with the actor's control over interoperability elements. As an example, a dominant health IT developer of certified health IT or network that refuses to facilitate a particular form of access, exchange, or use with other entities would have to demonstrate an extreme burden relative to the need for access, exchange, or use in order to qualify for this exception. This exacting standard would also apply in other circumstances of dependence or reliance on the actor to facilitate access, exchange, or use. For example, a dominant health system that provides local health IT infrastructure would have to demonstrate an extreme hardship to justify denying interconnection requests or access to interoperability elements. Likewise, where the actor is a business associate of a covered entity, or owes some other special duty to the requestor, the actor could not qualify for this exception unless the cost or burden it would have borne was so extreme in comparison to the marginal benefits to the requestor that the request was clearly unreasonable by any objective measure.

We acknowledge that there may be situations when complying with a request for access, exchange, or use would be considered infeasible because an actor is unable to provide such access, exchange, or use due to unforeseeable or unavoidable circumstances that are outside the actor's control. For example, an actor could seek coverage under this exception if it is unable to provide access, exchange, or use of EHI due to a natural disaster (such as a hurricane, tornado or earthquake) or war. These are just a couple examples of such circumstances and are by no means an exhaustive list.

We emphasize that, consistent with the requirements for demonstrating that activities and practices meet the conditions of an exception proposed in section VIII.C.6.c of this preamble, the actor would need to produce evidence and ultimately prove that complying with the request for access, exchange, or use in the manner requested would have imposed a clearly unreasonable burden on the actor under the circumstances.

We note that there are certain circumstances that we propose would not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether complying with a request would have been infeasible. We propose that it would not be considered a burden if providing the requested access, exchange, or use in the manner requested would have (1) facilitated competition with the actor; or (2) prevented the actor from charging a fee. Throughout this proposed rule, we have highlighted that one of the goals of the information blocking section is to promote competition, and allowing the argument that a request is infeasible because it facilitates competition with the actor would be antithetical to this goal. Similarly, an argument that a request is infeasible because it prevents the actor from charging a fee would also be outside the scope of this exception because such a result would not constitute a substantial, unreasonable burden that this exception seeks to address.

We request comment on the structured, fact-based approach we have proposed for determining whether a request was in fact ''infeasible'' within the meaning of this exception. We encourage comment on, among other issues, whether the factors we have specifically delineated above properly focus the infeasibility inquiry; whether our approach to weighing these factors is appropriate; and whether there are additional burdens, distinct from the immediate and direct financial and operational challenges contemplated above, that are similarly concrete and should be considered under the fact-based rubric of this exception.

ii. Duty to Timely Respond and Provide Reasonable Cooperation

In addition to demonstrating that a particular request or class of requests was infeasible, we propose that an actor would have to show that it satisfied several additional conditions. Specifically, to qualify for this exception, the actor must have timely responded to all requests relating to access, exchange, and use of EHI, including but not limited to requests to establish connections and to provide interoperability elements. Further, for any request that the actor claims was infeasible, the actor must have provided the requestor with a detailed written explanation of the reasons why the actor could not accommodate the request. Finally, the actor must have worked with the requesting party in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI, as applicable. The actor's failure to meet any of these conditions would disqualify the actor from the exception and could also be evidence that the actor knew that it was engaging in practices that contravened the information blocking provision.

We clarify that the duty to timely respond and provide reasonable cooperation would necessarily be assessed from the standpoint of what is objectively reasonable for an individual or entity in the actor's position. For example, we would not expect a small physician practice to provide the same level of engagement and technical assistance to third parties as a large hospital or health system with considerable health IT resources and expertise at its disposal. In some circumstances, it may even be difficult for a small practice to comply with any request for access, exchange, and use that is more complicated than a simple request for a patient's personal health information. If there are such requests—and there could be—then small practices may be both unable to comply with such requests and poorly situated to assist requesting parties with alternatives. We provide these examples to emphasize that we will look at the specific facts and circumstances of each case to determine what is objectively reasonable.

We believe that these conditions will minimize the risk that this exception could protect improper refusals to provide interoperability elements, including naked refusals to deal as well as other practices, such as improper delays in access or exchange that would present information blocking concerns. Additionally, the requirements for an actor to timely respond and document its justifications for declining a request in writing would prevent an actor from using post hoc rationalizations to justify these and other improper practices. Finally, we believe that establishing a clear duty under the exception for actors to deal on reasonable terms with parties seeking to access, exchange, or use EHI will encourage parties to cooperate to identify and implement efficient solutions to interoperability challenges, thereby avoiding disputes that could lead to information blocking.

We encourage comment on the additional conditions and related considerations described above. Specifically, we request comment regarding potential obstacles to satisfying these conditions and improvements we could make to the proposed process.

6. Licensing of Interoperability Elements on Reasonable and Non-Discriminatory Terms

We propose to establish an exception to the information blocking provision that would permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, provided that certain conditions are met. The exception and corresponding conditions are set forth in the proposed regulation text in § 171.206. As discussed in section VIII.C.5.a of this preamble, the information blocking provision would be implicated if an actor were to refuse to license or allow the disclosure of interoperability elements to persons who require those elements to develop and provide interoperable technologies or services—including those that might complement or compete with the actor's own technology or services. Moreover, the information blocking provision would be implicated if the actor licensed such interoperability elements subject to terms or conditions that have the purpose or effect of excluding or discouraging competitors, rivals, or other persons from engaging in these pro-competitive and interoperability-enhancing activities. Thus, this licensing requirement would apply in both vertical and horizontal relationships. For instance, it would apply when a developer in a vertical relationship to the actor—a network in this example—wants to use interoperability elements in order to access the EHI maintained in the actor's network. The requirement would also apply when a rival network in a horizontal relationship to the actor (network) wants to use interoperability elements so that its network can be compatible with the applications that have already been developed for use with the actor's network.

We note that some licensees do not require the interoperability elements to develop products or services that can be interoperable with the actor's health IT. For instance, there may be firms that simply want to license the actor's technology for use in developing their own interoperability elements. Their interest would be for access to the technology itself—not for the use of the technology to interoperate with either the actor or its customers. This may be the case, for example, if the relevant intellectual property included patents that were applicable to other information technology applications outside of health IT. In such cases, the actor's licensing of its patents in such a context would *not* implicate the information blocking provision.

Below are examples of situations that *would implicate* the information blocking provision (these examples are not exhaustive):

- An actor refuses to negotiate a license after receiving a request from a developer.
- An actor offers a license at the request of a developer, but only at a royalty rate that exceeds a RAND rate.
- An actor offers a license to a competitor at a royalty rate significantly higher than was offered to a party not in direct competition with the actor.
- An actor files a patent infringement lawsuit against a developer without first offering to negotiate a license on RAND terms.

There are compelling reasons for this prohibition. In our experience, contractual and intellectual property rights are frequently used to extract rents for access to EHI or to prevent competition from developers of interoperable technologies and services (*see* section VIII.C.5.c.iv. of this preamble). These practices frustrate access, exchange, and use of EHI and stifle competition and innovation in the health IT sector. As a case in point, even following the enactment of the Cures Act, some EHR developers are selectively prohibiting—whether expressly or through commercially unreasonable terms—the disclosure or use of technical interoperability information required for third-party applications to be able to access, exchange, and use EHI maintained in EHR systems. This limits health care providers' use of the EHI maintained on their behalf to the particular capabilities and use cases that their EHR developer happens to support. More than this, by limiting the ability of providers to choose what applications and technologies they can use with their EHR systems, these practices close off the market to innovative applications and services that providers and other stakeholders need to deliver greater value and choice to health care purchasers and consumers.

Despite these serious concerns, we recognize that the definition of information blocking may be broader than necessary and could have unintended consequences. In contrast to the practices described above, we believe it is generally appropriate for actors to license their intellectual property (IP) on RAND terms that do not block interoperability. Provided certain conditions are met, we believe that these practices would further the goals of the information blocking provision by allowing actors to protect the value of their innovations and earn returns on the investments they have made to develop, maintain, and update those innovations. This in turn will protect future incentives to invest in, develop, and disseminate interoperable technologies and services. Conversely, if actors cannot (or believe they cannot) protect and commercialize their innovations, they may not engage in these productive activities that improve access, exchange, and use of EHI.

While we believe this exception is necessary to promote competition and consumer welfare, we are highly sensitive to the danger that actors will continue to use their contractual and IP rights to interfere with access, exchange, and use of EHI, undermining the information blocking provision's fundamental objectives. For this reason, the exception would be subject to strict conditions to ensure, among other things, that actors license interoperability elements on RAND terms and that they do not impose collateral terms or engage in other practices that would impede the use of the interoperability elements or otherwise undermine the intent of this exception.

We acknowledge that preventing intellectual property holders from extracting rents for access to EHI may differ from standard intellectual property policy. Absent specific circumstances, IP holders are generally free to negotiate with prospective licensees to determine the royalty to practice their IP, and this negotiated royalty frequently reflects the value the licensee would obtain from exercising those rights. However, in the context of EHI, we propose that a limitation on rents is essential due to the likelihood that rents will frustrate access, exchange, and use of EHI, particularly because of the power dynamics that exist in the health IT market.

We remind readers that actors are not required to seek the protection of this (or any other) exception. If an actor does not want to license a particular technology, it may choose to comply with the information blocking provision in another way, such as by developing and providing alternative means of accessing, exchanging, and using EHI that are similarly efficient and efficacious. The purpose of this exception is not to dictate a licensing scheme for all, or even most, health IT, but rather to provide a tailored ''safe harbor'' that will provide clear expectations for those who desire it.

i. Reasonable and Non-Discriminatory (RAND) Terms

We propose to require, as a condition of this exception, that any terms upon which an actor licenses interoperability elements must be reasonable and non-discriminatory (RAND). As discussed below, commitments to license technology on RAND terms are frequently required in the context of standards development organizations (SDOs), and we believe that the practical and policy considerations that have led SDOs to adopt these policies are related in many respects to the information blocking concerns presented when an actor exploits control over interoperability elements to extract economic rents or impede the development or use of interoperable technologies and services.

We recognize that strong legal protections for IP rights can promote competition and innovation.[125] Nevertheless, IP rights can also be misused in ways that undermine these goals.[126] We believe this potential for abuse is heightened when the IP rights pertain to functional aspects of technology that are essential to enabling interoperability. As an important example, a technology developer may encourage the inclusion of its technology in an industry standard created by an SDO while not disclosing that it has IP rights in that technology. After the SDO incorporates the technology into its standard, and industry begins to make investments tied to the standard, the IP-holder may then assert its IP rights and demand royalties or license terms that it could not have achieved before the standard was adopted because companies would incur substantial switching costs to abandon initial designs or adopt different products.[127] To address these

[125] *See* FTC and DOJ Antitrust Guidelines for the Licensing of Intellectual Property, at 2 (2017), *https://www.ftc.gov/system/files/documents/public_statements/1049793/ip_guidelines_2017.pdf.*

[126] *See Assessment Techs. of WI, LLC* v. *WIREdata, Inc.,* 350 F.3d 640, 644–45 (7th Cir. 2003); *Sega Enterprises Ltd.* v. *Accolade, Inc.,* 977 F.2d 1510, 1520–28 (9th Cir. 1992); *Sony Computer Entertainment, Inc.* v. *Connectix Corp.,* 203 F.3d 596, 602–08 (9th Cir. 2000); *Bateman* v. *Mnemonics, Inc.,* 79 F.3d 1532, 1539–40 n. 18 (11th Cir. 1996); *Atari Games Corp.* v. *Nintendo of America, Inc.,* 975 F.2d 832, 842–44 (Fed. Cir. 1992).

[127] *See* DOJ and FTC, Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition, at 37–40 (Apr. 2017), *https://www.ftc.gov/sites/default/files/documents/reports/antitrust-enforcement-and-intellectual-property-rights-promoting-innovation-and-competition-report.s.department-justice-and-federal-trade-commission/p040101promotinginnovationandcompetitionrpt0704.pdf.*

types of concerns, while balancing the legitimate interests and incentives of IP owners, many SDOs now have policies requiring members who contribute technologies to a standard to voluntarily commit to license that technology on RAND terms and will consider whether firms have made voluntary RAND commitments when weighing whether to include their technology in standards.[128] While this commitment to license on RAND terms is voluntary as compared to our proposed requirement to use RAND terms, it serves to illustrate how RAND terms can be used to address such concerns.

Similar concerns arise when actors who control proprietary interoperability elements demand royalties or license terms from competitors or other persons who are technologically dependent on the use of those interoperability elements. As discussed in section VIII.C.5 of this preamble, to the extent that the interoperability elements are essential to enable the efficient access, exchange, or use of EHI by particular persons or for particular purposes, any practice by the actor that could impede the use of the interoperability elements for that purpose—or that could unnecessarily increase the cost or other burden of using the elements for that purpose—would give rise to an obvious risk of interference with access, exchange, or use of EHI under the information blocking provision.

We believe that a RAND requirement would balance the need for robust IP protections with the need to ensure that this proposed exception does not permit actors to exercise their IP or other proprietary rights in inappropriate ways that block the development, adoption, or use of interoperable technologies and services. The exercise of IP rights in these ways is incompatible with the information blocking provision, which protects the investments that taxpayers and the health care industry have made to adopt technologies that will enable the efficient sharing of EHI to benefit consumers and the health care system. While actors are entitled to protect and exercise their IP rights, to benefit from this exception to the information blocking provision they must do so in a reasonable and non-discriminatory manner that does not undermine these efforts and impede the appropriate flow of EHI.

Accordingly, we propose that, to qualify for this exception, an actor must license requested interoperability elements on RAND terms. To comply with this condition, any terms or conditions under which the actor discloses or allows the use of interoperability elements must meet several requirements set forth below. These requirements apply to both price terms (such as royalties and license fees) and other terms, such as conditions or limitations on access to interoperability elements or the purposes for which they can be used.

Responding To Requests

We propose that, upon receiving a request to license or use interoperability elements, an actor would be required to respond to the requestor within 10 business days from receipt of the request. We note that the request could be made to ''license'' or ''use'' the interoperability elements because a requestor may not always know that ''license'' is the legal mechanism for ''use'' when making the request. This provision is intended to ensure that a requestor is given an opportunity to license *and* use interoperability elements. As such, the requirement for responding to requests should not be limited to requests to ''license.''

In order to meet this requirement, the actor would be required to respond to the requestor within 10 business days from the receipt of the request by: (1) Negotiating with the requestor in a RAND fashion to identify the interoperability elements that are needed; and (2) offering an appropriate license with RAND terms, consistent with its other obligations under this exception. We emphasize that, in order to qualify for this proposed exception, the actor is only required to *negotiate* with the requestor in a RAND fashion and to *offer* a license with RAND terms. The actor is not required to *grant* a license in all instances. For example, the actor would not be required to grant a license if the requestor refuses an actor's offer to license interoperability elements on RAND terms.

We emphasize that there would be circumstances under which the actor could pursue legal action against parties that infringe its intellectual property whilst complying with this exception. For instance, an actor could bring legal action if a firm appropriates the actor's intellectual property without requesting a license or after refusing to accept a license on RAND terms.

We do not propose a set timeframe for when the negotiations must be resolved because it is difficult to predict the duration of such negotiations. For instance, there could be situations when the actor and requestor meet once and the actor makes a RAND offer that is immediately accepted by the requestor. However, there could be other situations when the requestor and actor each make counteroffers, which would extend the negotiations.

We request comment on whether 10 business days is an appropriate amount of time for the actor to respond to the requestor. In proposing this timeframe, we considered the urgency of certain requests to license interoperability elements and our expectation that developers would have standard licenses at their disposal that could be adapted in these situations. We considered proposing response timeframes ranging from 5 business days to 15 business days. We also considered proposing two separate timeframes for: (1) Negotiating with the requestor; and (2) offering the license. If commenters prefer a different response timeframe or approach than proposed, we request that commenters explain their rationale with as much detail as possible.

In addition, we query whether we should create set limits for: (1) The amount of time the requestor has to accept the actor's initial offer or make a counteroffer; (2) if the requestor makes a counteroffer, the amount of time the actor has to accept the requestor's counteroffer or make its own counteroffer; and (3) an allowable number of counteroffers in negotiations.

Scope of Rights

To qualify for this proposed exception, we propose that the actor must license the requested interoperability elements with all rights necessary to access and use the interoperability elements for the following purposes, as applicable:

- All rights necessary to access and use the interoperability elements for the purpose of developing products or services that are interoperable with the actor's health IT or with health IT under the actor's control and/or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control. These rights would include the right to incorporate and use the interoperability elements in the licensee's own technology to the extent necessary to accomplish this purpose.
- All rights necessary to market, offer, and distribute the interoperable products and services described above to potential customers and users, including the right to copy or disclose the interoperability elements as necessary to accomplish this purpose.
- All rights necessary to enable the use of the interoperable products or services in production environments,

[128] *See, e.g., Microsoft Corp.* v. *Motorola, Inc.,* No. C10–1823JLR, 2013 WL 2111217, at *6 (W.D. Wash. Apr. 25, 2013).

including using the interoperability elements to access and enable the exchange and use of electronic health information.

We request comment on whether these rights are sufficiently inclusive to support licensees in developing interoperable technologies, bringing them to market, and deploying them for use in production environments. We also request comment on the breadth of these required rights and if they should be subject to any limitations that would not interfere with the uses we have described above.

Reasonable Royalty

As a condition of this exception, we propose that if an actor charges a royalty for the use of interoperability elements, the royalty base and rate must be reasonable. Consistent with the requirements for demonstrating that activities and practices meet the conditions of an exception proposed in section VIII.C.6.c, the actor would need to show that the royalty base was reasonable and that the royalty was within a reasonable range for the interoperability elements at issue. Importantly, we note that the reasonableness of any royalties would be assessed solely on basis of the independent value of the actor's technology to the licensee's product,[129] *not* on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information. For instance, the reasonableness of royalties could not be assessed based on the strategic value stemming from the adoption of the technology by customers or users, the switching costs associated with the technology, or other circumstances of technological dependence described elsewhere in this preamble (see section VIII.C.5). We note that ''strategic value'' would stem from the actor's control over essential means of accessing, exchanging, or using electronic health information. Limiting a reasonable royalty to the value of the technology isolated from strategic value is similar in concept to apportionment of reasonable royalties for the infringement of standard essential patents (SEPs).[130] In our context, permitting an actor to charge a royalty on the basis of these considerations would effectively allow the actor to extract rents on access, exchange, and use of EHI, which is contrary to the goals of the information blocking provision.

In evaluating the actor's assertions and evidence that the royalty was reasonable, we propose that ONC may consider the following factors:

- The royalties received by the actor for the licensing of the proprietary elements in other circumstances comparable to RAND-licensing circumstances.
- The rates paid by the licensee for the use of other comparable proprietary elements.
- The nature and scope of the license.
- The effect of the proprietary elements in promoting sales of other products of the licensee and the licensor, taking into account only the contribution of the elements themselves and not of the enhanced interoperability that they enable.
- The utility and advantages of the actor's interoperability element over the existing technology, if any, that had been used to achieve a similar level of access, exchange, or use of EHI.
- The contribution of the elements to the technical capabilities of the licensee's products, taking into account only the value of the elements themselves and not the enhanced interoperability that they enable.
- The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the proprietary elements or analogous elements that are also covered by RAND commitments.
- The portion of the realizable profit that should be credited to the proprietary elements as distinguished from non-proprietary elements, the manufacturing process, business risks, significant features or improvements added by the licensee, or the strategic value resulting from the network effects, switching costs, or other effects of the adoption of the actor's technology.
- The opinion testimony of qualified experts.
- The amount that a licensor and a licensee would have agreed upon (at the time the licensee began using the elements) if both were considering the RAND obligation under this exception and its purposes, and had been reasonably and voluntarily trying to reach an agreement.

These factors mirror those used by courts that have examined the reasonableness of royalties charged pursuant to a commitment to an SDO to license standard-essential technologies on RAND terms (*see Microsoft Corp.* v. *Motorola, Inc.;*[131] In re *Innovatio IP Ventures, LLC Patent Litig.;*[132] and *Realtek Semiconductor Corp.* v. *LSI Corp*[133]). However, we have adapted the factors to the information blocking context as follows. In the SDO context, the RAND requirement mitigates the risk that patent-holders will engage in ''hold up''—that is, charging excessive royalties that do not reflect the value of their contributions to the standard, but rather reflect the costs associated with switching to alternative technologies after a standard is adopted—and that the cumulative effect of such royalties will make the standard too expensive to implement—a problem called ''royalty stacking.''[134] To address the risks of hold-up and royalty stacking in the standards development context, a RAND license should compensate a patentee for their technical contribution to the technology embodied in a standard, but should not compensate them for mere inclusion in the standard.

Similarly, in the context of information blocking, we propose the RAND inquiry focuses on whether the royalty demanded by the actor represents the independent value of the actor's proprietary technology. We propose that if the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies. Rather than asking whether the royalty inappropriately captures additional value derived from the technology's inclusion in the industry standard, we would ask whether the actor is charging a royalty that is not based on the value of its technology (embodied in the interoperability elements) but rather includes the strategic value stemming from the adoption of that technology by customers or users. Thus, under this proposed approach and the factors set forth above, we would consider the technical contribution of the actor's interoperability elements to the licensee's products—such as any proprietary capabilities or features that the licensee uses in its product—but would screen out any functional aspects of the actor's technology that are used only to establish interoperability and enable EHI to be accessed, exchanged, and used. Additionally, we propose that

[129] *See Ericsson, Inc.* v. *D-Link Systems, Inc.,* 773 F.3d 1201, 1226; 1232 (Fed. Cir. 2014).

[130] *See, e.g., Georgia-Pacific Corp.* v. *United States Plywood Corp.,* 318 F. Supp 1116 (S.D.N.Y. 1970) (utilizing the more common approach).

[131] Case No. 10–cv–1823 JLR, 2013 WL 2111217 (W.D.Wash. Apr. 25, 2013).

[132] MDL 2303, 2013 WL 5593609 (N.D.Ill. Oct. 3, 2013).

[133] Case No. 5:12–cv–03451–RMW, 2014 WL 46997 (N.D.Cal. Jan. 6, 2014).

[134] *Microsoft Corp.* v. *Motorola, Inc.,* 864 F.Supp.2d 1023, 1027 (W.D.Wash. 2012).

to address the potential risk of royalty stacking we would need to consider the aggregate royalties that would apply if owners of other essential interoperability elements made royalty demands of the implementer. Specifically, we propose that, to qualify for this exception, the actor must grant licenses on terms that are objectively commercially reasonable taking into account the overall licensing situation, including the cost to the licensee of obtaining other interoperability elements that are important for the viability of the products for which it is seeking to license interoperability elements from the actor.

We clarify that, as proposed, this condition would not preclude an actor from licensing its interoperability elements pursuant to an existing RAND commitment to an SDO. We also note that, in addition to complying with the requirements described above, to meet this proposed condition any royalties charged must meet the condition, proposed separately below, that any license terms be non-discriminatory.

We request comment on these aspects of the proposed exception. Commenters are encouraged to consider, in particular, whether the factors and approach we have described will be administrable and appropriately balance the unreasonable blocking by actors of the use of essential interoperability elements with the need to provide adequate assurance to investors and innovators that they will be able to earn a reasonable return on their investments in interoperable technologies. If our proposed approach does not adequately balance these concerns or would not achieve our stated policy goals, we ask that commenters suggest revisions or alternative approaches. We ask that such comments be as detailed as possible and provide rigorous economic justifications for any suggested revisions or alternative approaches.

Non-Discriminatory Terms

We propose that for this exception to apply the terms on which an actor licenses and otherwise provides interoperability elements must be non-discriminatory. This requirement would apply to both price and non-price terms, and thus would apply to the royalty terms discussed immediately above as well as other types of terms that may be included in licensing agreements or other agreements related to the provision or use of interoperability elements.

To comply with this condition, the terms on which the actor licensed the interoperability elements must be based on criteria that the actor applied uniformly for all substantially similar or similarly situated classes of persons and requests. This requirement addresses a root cause of information blocking. In order to be considered non-discriminatory, such criteria would have to be objective and verifiable, not based on the actor's subjective judgment or discretion. We emphasize that this proposal does not mean that the actor must apply the same terms for all persons or classes of persons requesting a license. However, any differences in terms would have to be based on actual differences in the costs that the actor incurred or other reasonable and non-discriminatory criteria. Moreover, we propose that any criteria upon which an actor varies its terms or conditions would have to be both competitively neutral—meaning that the criteria are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor—and neutral as to the revenue or other value that the requestor may be derived from access, exchange, or use of the EHI obtained via the interoperability elements, including any secondary use of such EHI. We believe these limitations are necessary in light of the potential for actors to use their control over interoperability elements to engage in discriminatory practices that create unreasonable barriers or costs for persons seeking to develop, offer, or use interoperable technologies to expand access and enhance the exchange and use of EHI.

To clarify our expectations for this proposed condition, we provide the following illustration. Consider an EHR developer that establishes an ''app store'' through which third-party developers can license the EHR developer's proprietary APIs, which we assume are separate from the APIs required by the API Condition of Certification proposed in § 170.404. The EHR developer could charge a reasonable royalty and impose other reasonable terms to license these interoperability elements. The terms and conditions could vary based on neutral, objectively verifiable, and uniformly applied criteria. These might include, for example, significantly greater resources consumed by certain types of apps, such as those that export large volumes of data on a continuous basis, or the heightened risks associated with apps designed to ''write'' data to the EHR database or to run natively within the EHR's user interface. In contrast, the EHR developer could *not* vary its terms and conditions based on subjective criteria, such as whether it thinks an app will be ''popular'' or is a ''good fit'' for its ecosystem. Nor could it offer different terms or conditions on the basis of objective criteria that are not competitively neutral, such as whether an app ''connects to'' other technologies or services, provides capabilities that the EHR developer plans to incorporate in a future release of its technology, or enables an efficient means for customers to export data for use in other databases or technologies that compete directly with the EHR developer. Similarly, the EHR developer could not set different terms or conditions based on how much revenue or other value the app might generate from the information it collects through the APIs, such as by introducing a revenue-sharing requirement for apps that use data for secondary purposes that are very lucrative and for which the EHR developer would like a ''piece of the pie.'' Such practices would disqualify the actor from this exception and would implicate the information blocking provision.

The foregoing conditions are not intended to limit an actor's flexibility to set different terms based on legitimate differences in the costs to different classes of persons or in response to different classes of requests, so long as any such classification was in fact based on neutral criteria (in the sense described above) that are objectively verifiable and were applied in a consistent manner for persons and/or requests within each class. As an important example, the proposed condition would not preclude a covered actor from pursuing strategic partnerships, joint ventures, co-marketing agreements, cross-licensing agreements, and other similar types of commercial arrangements under which it provides more favorable terms than for other persons with whom it has a more arms-length relationship. In these instances the actor should have no difficulty identifying substantial and verifiable efficiencies that demonstrate that any variations in its terms and conditions were based on objective and neutral criteria. We do note an important caveat, however, specifically that a health IT developer of certified health IT who is an ''API Technology Supplier'' under the Condition of Certification proposed in § 170.404 would not be permitted to offer different terms in connection with the APIs required by that Condition of Certification. As discussed in section VII.B.4 of this preamble, we propose that API Technology Suppliers are required to make these APIs available on terms that are no less favorable than provided to their own customers, suppliers, partners, and other persons with whom they have a business relationship. As noted below towards the end of our discussion of this exception to the information blocking provision, the exception incorporates the API Condition of Certification's requirements in full for all health IT developers subject to that condition.

We welcome comments on the foregoing condition and requirements.

Collateral Terms

We propose five additional conditions that would reinforce the requirements of this exception discussed above. These additional conditions would provide bright-line prohibitions for certain types of collateral terms or agreements that we believe are inherently likely to interfere with access, exchange, or use of EHI. We propose that any attempt to *require* a licensee or its agents or contractors to do or agree to do any of the following would disqualify the actor from this exception and would be suspect under the information blocking provision.

First, the actor must not require the licensee or its agents or contractors to not compete with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development. We are aware that such agreements have been used to either directly exclude suppliers of interoperable technologies and services from the market or to create exclusivity that reduces the range of technologies and options available to health care providers and other health IT customers and users.

Second, and for similar reasons, the actor must not require the licensee or its agents or contractors to deal exclusively with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development.

Third, the actor must not require the licensee or its agents or contractors to obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements. This condition reinforces the condition described earlier requiring that any royalties charged by the actor for the use of interoperability elements be reasonable. Without this condition, we believe that an actor could require a licensee to take a license to additional interoperability elements that the licensee does not need or want, which could enable the actor to extract royalties that are inconsistent with its RAND obligations under this exception. We clarify that this condition would not preclude an actor and a willing licensee from agreeing to such an arrangement, so long as the arrangement was not *required.*

Fourth, the actor must not condition the use of interoperability elements on a requirement or agreement to license, grant, assign, or transfer the licensee's own IP to the actor. We believe it is inconsistent with the actor's RAND licensing obligations under this exception, and would raise information blocking concerns, for an actor to use its control over interoperability elements as leverage to obtain a ''grant back'' of IP rights or other consideration whose value may exceed that of a reasonable royalty. Consistent with our approach under other conditions of this exception, this condition would not preclude an actor and a willing licensee from agreeing to a cross-licensing, co-marketing, or other agreement if they so choose. However, the actor cannot *require* the licensee to enter into such an agreement. The actor must offer the option of licensing the interoperability elements without a promise to provide consideration beyond a reasonable royalty. We note that in the SDO context, it can sometimes be consistent with RAND terms to require that an SEP licensee also grant a cross-license to any SEPs that it holds, provided that the cross-license is limited to patents essential to the licensed standard. In this way, this condition differs from licensing in the SDO context.

Finally, the actor must not condition the use of interoperability elements on a requirement or agreement to pay a fee of any kind whatsoever unless the fee meets either the narrowly crafted condition to this exception for a reasonable royalty, or, alternatively, the fee satisfies the separate exception proposed in § 171.204, which permits the recovery of certain costs reasonably incurred. As noted in section VIII.D.4, that exception generally does not allow for the recovery of royalties or other fees associated with intangible assets. However, the exception does allow for the reasonable and actual development and acquisition costs of such assets.

We request comment on the categorical exclusions outlined above. In particular, we encourage commenters to weigh in on our assumption that these practices are inherently likely to interfere with access, exchange, or use of EHI. We also encourage commenters to suggest any conceivable benefits that these practices might offer for interoperability or for competition and consumers that we might have overlooked. Again, we ask that to the extent possible commenters provide detailed economic rationale in support of their comments.

Non-Disclosure Agreement

We propose that an actor would be permitted under this exception to require a licensee to agree to a confidentiality or non-disclosure agreement (NDA) to protect the actor's trade secrets, provided that the NDA is no broader than necessary to prevent the unauthorized disclosure of the actor's trade secrets. Further, we propose that the actor would have to identify (in the NDA) the specific information that it claims as trade secrets, and that such information would have to meet definition of a trade secret under applicable law. We believe these safeguards are necessary to ensure that the NDA is not used to impose restrictions or burdensome requirements that are not actually necessary to protect the actor's trade secrets and that impede the use of the interoperability elements. The use of an NDA for such purposes would preclude an actor from qualifying for this exception and would implicate the information blocking provision. We note that if the actor is a health IT developer of certified health IT, it may be subject to the Condition of Certification proposed in § 170.403, which prohibits certain health IT developer prohibitions and restrictions on communications about a health IT developer's technology and business practices. This exception would not in any way abrogate the developer's obligations to comply with that condition.

We encourage comment on this condition of the proposed exception.

ii. Additional Requirements Relating to the Provision of Interoperability Elements

In addition to the conditions described above, we propose that an actor's practice would need to comply with additional conditions that ensure that actors who license interoperability elements on RAND terms do not engage in separate practices that impede the use of those elements or otherwise undermine the intent of this exception. These conditions are analogous to the conditions described in our proposal above concerning collateral terms but address a broader range of practices that may not be effected through the license agreements themselves or that occur separately from the licensing negotiations and other dealings between the actor and the licensee. Specifically, we propose that an actor would not qualify for this exception if it engaged in a practice that had the purpose or effect of impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose; or the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand. As an illustration, the exception would not apply if the developer licensed its proprietary APIs for use by third-party apps but then prevented or delayed the use of those apps in production environments by, for example, restricting or discouraging customers from enabling the use of the apps, or engaging in ''gate keeping'' practices, such as requiring apps to go through a vetting process and then applying that process in a discriminatory or unreasonable manner.

Finally, to ensure the actor's commitments under this exception are durable, we propose one additional safeguard: An actor cannot avail itself of this exception if, having licensed the interoperability elements, the actor makes changes to the elements or its technology that ''break'' compatibility or otherwise degrade the performance or interoperability of the licensee's products or services. We believe this condition is crucial given the ease with which an actor could make subtle ''tweaks'' to its technology or related services that could disrupt the use of the licensee's compatible technologies or services and result in substantial competitive and consumer injury.

We clarify and emphasize that this proposed condition would in *no way* prevent an actor from making improvements to its technology or responding to the needs of its own customers or users. However, to benefit from the exception, the actor's practice would need to be necessary to accomplish these purposes and the actor must have afforded the licensee a reasonable opportunity under the circumstances to update its technology to maintain interoperability. We also recognize that an actor may have to suspend access or make other changes immediately and without prior notice in response to legitimate privacy, security, or patient safety-related exigencies. Such practices would be governed by the exceptions proposed in section VIII.D of this preamble and thus would not need to qualify for this exception.

iii. Compliance With Conditions of Certification

As a final condition of this proposed exception, we propose that health IT developers of certified health IT who are subject to the Conditions of Certification proposed in §§ 170.402, 170.403, and 170.404 must comply with all requirements of those Conditions of Certification for all practices and at all relevant times. Several of the requirements of these conditions mirror those of this exception. However, in some instances the Conditions of Certification provide additional or more specific requirements that apply to the provision of interoperability elements by developers of certified health IT. For example, developers subject to the API Condition of Certification must make certain public APIs available on terms that are royalty free and no less favorable than provided to themselves and their customers, suppliers, partners, and other persons with whom they have a business relationship. These more prescriptive requirements reflect the specific obligations of health IT developers under the Program, including the duty to facilitate the access, exchange, and use of information from patients' electronic health records without special effort. A health IT developer of certified health IT's failure to comply with these and other certification requirements that specifically support interoperability would, in addition to precluding the developer from invoking this exception, be significant evidence of information blocking.

7. Maintaining and Improving Health IT Performance

We propose to establish an exception to the information blocking provision for certain practices that are reasonable and necessary to maintain and improve the overall performance of health IT, provided certain conditions are met. The proposed exception would recognize as reasonable and necessary the practice of an actor making health IT under its control temporarily unavailable to maintain or improve the health IT. The exception and corresponding conditions are set forth in the proposed regulation text in § 171.207.

EHI should be accessible and usable on demand by those that need it. However, in order for this to happen, the health IT through which EHI is accessed, exchanged, or used must perform properly and efficiently. This requires that health IT be maintained and in some instances improved. The performance of such maintenance and improvements sometimes requires that health IT is temporarily taken offline, which can interfere with the access, exchange, and use of EHI. We believe this exception is necessary to ensure that actors are not deterred from maintaining and improving the overall performance of health IT because temporary unavailability of EHI may cause interference with its access, exchange, and use. Without this specific exception, there could be a significant risk that actors may refrain from conducting maintenance and improvements of health IT out of fear that if the purpose was not for preventing harm, promoting security, or for another reason covered by the other exceptions, then their actions might contravene the information blocking provision.

This exception would apply to the unavailability of health IT occasioned by both planned and unplanned maintenance and improvements. Planned maintenance or improvements are typically carried out at regular intervals and address routine repairs, updates, or new releases. Unplanned maintenance or improvements respond to urgent or time-sensitive issues, which cannot wait for the occurrence of a pre-planned time period to implement the required maintenance or improvements.

This proposed exception acknowledges that the performance of health IT is often measured by service level agreements that provide flexibility to ensure that system availability is balanced with essential maintenance and improvements. Where the provision of health IT is subject to an allowance for maintenance or improvement that has been agreed to by the recipient of that health IT, we propose that neither that agreement, nor the performance of it, should constitute information blocking, provided that certain conditions are met.

To ensure that the actor's practice of making health IT, and in turn EHI, unavailable for the purpose of carrying out maintenance or improvements is reasonable and necessary, we have identified conditions that must be satisfied at all relevant times to qualify for this exception.

Unavailability of Health IT Must Be for no Longer Than Necessary To Achieve the Maintenance or Improvements for Which the Health IT was Made Unavailable

Any unavailability of health IT must be for a period of time no longer than necessary to achieve the maintenance or improvement purpose for which the health IT is made unavailable. This condition recognizes the critical importance of access to EHI and ensures that health IT is not made unavailable for longer than needed. For example, a health IT developer of certified health IT that has the right under its contract with a large health system to take its system offline for four hours each month to conduct routine maintenance would not qualify for this exception if an information blocking claim was made about a period of unavailability during which no maintenance was performed.

Making this evaluation for unplanned maintenance or improvements will be more difficult, because unplanned maintenance or improvements are typically initiated in response to a threat or risk that needs to be responded to on an urgent basis and for so long as the threat or risk persists. However, if, for example, an HIE identified a software failure (not identified as a safety or security risk) that required immediate remediation necessitating the actor take its health IT offline, the actor would be expected to bring the health IT back online as soon as possible after the issue was resolved.

Unavailability of Health IT for Maintenance or Improvements Must Be Implemented in a Consistent and Non-Discriminatory Manner

We propose that any unavailability of health IT occasioned by the conduct of maintenance or improvements must be implemented in a consistent and non-discriminatory manner. This condition provides a basic assurance that when health IT is made unavailable for the purpose of performing maintenance or improvements that the unavailability is not abused by the actor that controls the health IT. For example, a health IT developer of certified health IT would not qualify for this exception if the developer, using a standard contract that provided a flexible allowance for planned maintenance or improvements, initiated planned maintenance or improvements for a customer with an expiring health IT contract during a time when users might reasonably be expected to access EHI, but conducted planned maintenance or improvements for new customers in the middle of the night. However, this condition does not require that actors conduct planned maintenance or improvements simultaneously, or require that every health IT contract provide the same promises in regard to planned maintenance or improvements. Indeed, a recipient of health IT may agree to a longer window for unavailability in exchange for a reduced fee for system maintenance, which would not contravene this condition.

Unavailability of Health IT for Maintenance or Improvements Must Be Agreed

In order to benefit from this exception, we propose that the unavailability of health IT due to maintenance or improvements initiated by a health IT developer of certified health IT, HIE, or HIN, must be agreed to by the individual or entity to whom the health IT is supplied. The availability of health IT is typically addressed in a written contract or other written agreements, that puts the recipient of the health IT on notice about the level of EHI and health IT unavailability that can be expected for users of the health IT. By such agreements, the recipient of the health IT willfully agrees to that level of planned and unplanned unavailability (typically referred to in health IT contracts as ''downtime''). Some health IT contracts address the question of system availability by way of an ''uptime warranty'' that specifies the maximum amount of unavailability for a specified period and the timing of any planned unavailability.

We acknowledge that in some cases, health IT needs to be taken offline or maintenance or improvements on an urgent basis and in a way that is not expressly permitted under a health IT contract. An actor may still satisfy this proposed condition so long as the maintenance or improvements are agreed to by the recipient of the health IT. This could be achieved by way of an oral agreement reached between the parties by telephone, but we note that because an actor must demonstrate that it satisfies the requirements of this exception, it would be best practice for an actor to ensure the agreement was in writing or, at minimum, contemporaneously documented.

This proposed condition of this exception only applies when the unavailability of health IT is caused by a health IT developer of certified health IT, HIE, or HIN. In these circumstances, it is the supplier of the health IT that controls if and when health IT is intentionally taken offline for maintenance or improvements. This condition does not apply when health IT is made unavailable for maintenance or improvements at the initiative of a recipient (or customer) of health IT, because in that case, the unavailability has, for the purpose of this exception, nothing to do with the supplier. When it is a customer of health IT that initiates unavailability, the unavailability would not need to be the subject of an agreement with the supplier of that health IT, nor anyone else, in order for the customer of health IT to benefit from this exception. For example, a health care provider that locally hosts and maintains its health IT (being software supplied by a health IT developer) would not need to satisfy this condition if it interfered with access to EHI by taking the health IT offline temporarily to conduct maintenance. However, if the same health care provider was to receive a new release of the health IT developer's software, which was to be implemented by the developer and which required that the health IT be taken offline by the developer for 6 hours, then that unavailability, or an allowance for it, would need to be the subject of prior agreement. Unavailability of health IT initiated by a recipient of health IT (rather than the supplier of the health IT) would still need to satisfy the other conditions of this exception, including that the unavailability be for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable.

We note that this condition would need to be satisfied by any HIE or HIN that sought to benefit from this exception in connection with any interference with access, exchange, or use occasioned by an HIE or HIN making its health IT unavailable for the purposes of conducting maintenance or improvements. An HIE would need to have secured the agreement of those individuals or entities that use its exchange services, and a HIN would need to have obtained the agreement of the network's participants.

Interaction With Preventing Harm and Promoting Security Exceptions

When health IT is made unavailable for maintenance or improvements aimed at preventing harm to a patient or other person, or securing EHI, an actor must comply with the conditions specified in proposed § 171.201 or § 171.203 respectively, in order to qualify for an exception to the information blocking provision. This condition ensures that this exception cannot be used to avoid compliance with conditions applicable under other exceptions. For example, if part of an EHR system was taken offline in response to a health IT developer of certified health IT being alerted to the risk of corrupt or inaccurate data being recorded or incorporated in a patient's health record, any decision to make the EHR unavailable on this basis to conduct unplanned maintenance or improvements would need to accord with the conditions of the proposed exception for preventing harm (see § 171.201 and section VIII.D.1 of this proposed rule). Similarly, unavailability occasioned by maintenance or improvements initiated to secure EHI in response to a suspected malware attack would need to either be implemented in accordance with the actor's organizational security policy that satisfied the requirements of the proposed exception for promoting the security of EHI or if the practice did not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, consistent with the requirements of the exception (see § 171.203(d) and section VIII.D.3 of this proposed rule).

Request for Comment

We seek comment on this exception generally. Specifically, we seek comment on whether the proposed conditions impose appropriate limitations on actor-initiated health IT maintenance or improvements that lead to EHI unavailability. Our goal is to ensure that the exception is not abused, while at the same time recognizing reasonable commercial arrangements entered into by parties for the proper maintenance and improvement of health IT.

We are also considering whether to expand this exception to capture a broader class of practices that are the subject of reasonable commercial agreements and which, in the absence of an exception, may be considered information blocking. That is, to extend this exception or create new exceptions for additional types of practices that interfere with access, exchange, or use of EHI, but that are the subject of free agreement and which are reasonable and necessary. For example, we are considering whether a practice taken by an actor to throttle or meter the availability or performance of health IT, where agreed to by the recipient of that health IT, could ever be a practice that we recognize as not being information blocking if such practice does not otherwise qualify under an existing exception.

As discussed in section VIII.C.5 of this preamble, we are aware that actors can use commercial agreements to materially discourage, and in some instances outright prohibit, certain instances of access, exchange, or use of EHI. For example, a HIN might use a participation agreement to prohibit entities that receive EHI through the HIN from transmitting that EHI to entities who are not participants of the HIN. Such an arrangement would not be reasonable or necessary because there is no legitimate justification for it. However, we are also aware of commercial arrangements that are not motivated by anti-competitive considerations but that nonetheless have the effect of interfering with the access, exchange, or use of EHI. For example, a health IT developer of certified health IT may agree to commercial terms with a customer that have the effect of interfering with access, exchange, or use of EHI, but which are designed to appropriately accommodate the customer's limited resources, or to assure the performance of certain health IT functionality.

We expect that most reasonable and necessary commercial arrangements that affect access, exchange, or use of EHI could be recognized under one or more of the existing exceptions. However, we seek comment on whether there exists a class of legitimate commercial arrangements that could implicate the information blocking provision, but which would not benefit from the existing proposed exceptions.

E. Additional Exceptions—Request for Information

1. Exception for Complying With Common Agreement for Trusted Exchange

To support full network-to-network exchange of EHI, section 3001(c)(9)(A) of the PHSA, added by section 4003 of the Cures Act, directs the National Coordinator to convene public-private partnerships to develop or support a trusted exchange framework (Trusted Exchange Framework), including a common agreement for a common set of rules for trusted exchange between HINs (Common Agreement). The most recent draft Trusted Exchange Framework was released for public comment on January 5, 2018,[135] however, a new draft will be released in the coming months.

We are considering whether we would should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement. Such an exception may support adoption of the Common Agreement and encourage other entities to participate in trusted exchange through HINs that enter into the Common Agreement. It would do so by providing protection if there are practices that are expressly required by the Common Agreement, or that are necessary to implement such requirements, that might implicate the information blocking provision and would not qualify for another exception. We note that such an exception would be consistent with the complementary roles of the information blocking provision and other provisions of the Cures Act that support interoperability and enhance the trusted exchange of EHI (including the interoperable network exchange provisions at section 3001(c)(9) of the PHSA, the definition of interoperability at section 3000(10) of the PHSA, and the conditions of certification required by section 3001(c)(5)(D) of the PHSA).

We expect that any proposal would be narrowly framed such that contract terms, policies, or other practices that are not strictly necessary to comply with the Common Agreement would not qualify for the exception. Similarly, we expect that the proposal would provide that an actor could benefit from this exception only if the practice or practices that the actor pursued were no broader than necessary under the circumstances. These limitations would ensure that the exception is narrowly tailored to practices that are most likely to promote trusted exchange without unnecessarily impeding access, exchange, or use of EHI.

We ask commenters to provide feedback on this potential exception to the information blocking provision to be considered for inclusion in future rulemaking. Commenters should consider whether such an exception is necessary, given the scope of the other exceptions proposed in this NPRM, and whether there could be any negative effects of such an exception. We ask commenters to consider the appropriate scope of this exception, which could include which actors could benefit from the exception and the conditions that should apply in order to qualify for the exception.

2. New Exceptions

We welcome comment on any potential new exceptions we should consider for future rulemaking. Commenters should consider the policy goals and structure of the proposed exceptions in this proposed rule when providing comment. We ask that commenters provide rationale for any proffered exceptions to the information blocking provisions and any conditions an actor would need to meet to qualify for the proffered exception.

F. Complaint Process

Section 3022(d)(3)(A) of the PHSA directs the National Coordinator to implement a standardized process for the public to submit reports on claims of health information blocking. Such reports could be submitted regarding any practice by health care providers, health IT developers, exchanges, or networks that may constitute information blocking under section 3022(a). These practices include, but are not limited to, health IT products or developers of such products (or other entities offering such products to health care providers) not being interoperable or resulting in information blocking;

[135] ONC, *Draft Trusted Exchange Framework, https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.*

and false statements by developers of certified health IT that they have not engaged in information blocking. Section 3022(d)(3)(B) further requires that this complaint process provide for the collection of such information as the originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information.

We intend to implement and evolve this complaint process by building on existing mechanisms, including the complaint process currently available at *https://www.healthit.gov/healthit-feedback.* However, we request comment on this approach and any alternative approaches that would best effectuate this aspect of the Cures Act. In addition to any other comments that the public may wish to submit, we specifically request comment on the following issues:

- What types of information are most important to collect in order to identify potential instances of information blocking?
- What types of information are contemplated by the following categories delineated in section 3022(d)(3)(B): The originating institution; location; type of transaction; system and version; timestamp; terminating institution; locations; system and version; failure notice; and other related information?
- What types of information or data elements should be collected under each of the above categories?
- What additional types of information beyond the above may be relevant to complaints and allegations of information blocking, especially practices that involve contractual or other business practices for which some of the categories of technical or transactional information above may not apply?
- How can ONC encourage and streamline the collection of such information so as to minimize burden and encourage the submission of complaints, especially complaints about practices that raise the types of information blocking concerns described in this proposed rule?
- How can ONC facilitate the inclusion of sufficient detail and granularity in complaints to enable effective investigations?
- What safeguards should be provided to support adequate confidentiality and handling of information that could: (1) Identify the source of the complaint or allegation; (2) contain other individually identifiable information; and (3) contain confidential or proprietary business information?

G. Disincentives for Health Care Providers—Request for Information

Section 3022(b)(2)(B) of the PHSA provides that any health care provider determined by the OIG to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable federal law, as the Secretary sets forth through notice and comment rulemaking. However, we note that these disincentives may not cover the full range of conduct within the scope of section 3022(a)(1). We request information on disincentives or if modifying disincentives already available under existing HHS programs and regulations would provide for more effective deterrents.

We also seek information on the implementation of section 3022(d)(4) of the PHSA, which provides that in carrying out section 3022(d) of the PHSA, the Secretary shall, to the extent possible, not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved as of the day before December 13, 2016—enactment of the Cures Act.

IX. Registries Request for Information

Section 4005 (a) and (b) of the Cures Act focuses on interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. ONC is approaching these provisions from several angles to address the technical capability of EHRs to exchange data with registries in accordance with applicable recognized standards. Based on stakeholder engagement and public comments on prior ONC regulations, we have identified a wide range of areas where the use of standards could significantly improve bidirectional exchange with registries for a range of purposes, including public health, quality reporting, and care quality improvement.

As discussed in the ''Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs'' draft report released by ONC for public comment in December of 2018,[136] health care providers are faced with a myriad of federal public health reporting requirements and options that rely on both bidirectional exchange and aggregation of clinical data. CDC, SAMHSA, FDA, HRSA, and USDA also fund state and local public health jurisdictions to collect clinical data from health care providers. As noted in the Cures Act, there are also a wide range of clinician-led quality and specialty clinical data registries. Compounding these reporting requirements and options is, as reported by health care providers, a lack of standardization across electronic infrastructure that has led to a comparatively slow adoption of health IT systems among registries. This lack of interoperability impacts not only data exchange between health care providers, but is a significant barrier to the integration and potential use of clinical data received from a registry for quality improvement or clinical care.

For these reasons outlined above, we believe it is appropriate to explore multiple approaches to advancing health IT interoperability for bidirectional exchange with registries in order to mitigate risks based on factors like feasibility and readiness, potential unintended burden on health care providers, and the need to focus on priority clinical use cases. ONC is in the process of conducting research and analysis to determine what evidence-based use cases should be supported and what standards are available to support such use cases. We are also considering the overall maturity of technology adoption within the market to support identified standards and the use of certified EHRs and clinical data registries for these identified use cases in the near term, as well as identifying glide paths for the potential future development of enterprise solutions.

In the 2015 Edition final rule, we included certification criteria and standards that are applicable for specific use cases for bidirectional exchange such as Immunization Information Systems. In this proposed rule, we have proposed processes for updating standards as well as new policies related to real world testing that would help ensure that functionalities are implemented in a manner that is technically feasible in a practice setting. In addition, we have worked with federal partners to advance health IT policies related to bidirectional exchange with registries in a manner that supports and reflects the current market place while encouraging innovation and increased adoption. For example, we have worked with CMS to enhance guidance for QCDRs under the MIPS to support health IT innovation and partnership with health IT organizations. We are also working with the CDC and states to support enhancements to PDMP integration as a

[136] *https://www.healthit.gov/topic/usability-and-provider-burden/strategy-reducing-burden-relating-use-health-it-and-ehrs.*

priority use case for standards-based health IT solutions. We believe these efforts can help to address the near term need to support high priority use cases for bidirectional exchange between health care providers and registries.

In this proposed rule, we propose to adopt new standards and capabilities for certified APIs that have the potential to change how certain types of information exchange are done, including the potential to exchange information with clinical data and public health registries. In this request for information (RFI), we are seeking information on how health IT solutions and the proposals throughout this rule can aid bidirectional exchange with registries for a wide range public health, quality reporting, and clinical quality improvement initiatives. For example, in December of 2018, in the ''Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs'' draft report, we noted that HL7 was working on an update to the FHIR standard to support API access to request data on populations of patients, which could potentially address additional use cases, including supporting payer needs, public health and quality improvement efforts, and health research organizations. As discussed in section VII.4, FHIR Release 4 has now been published [85] and updated associated implementation specifications are expected to follow. FHIR Release 4 has several key improvements, including certain foundational aspects in the standard and ''FHIR resources'' designated as ''normative'' for the first time. This will lead to a cycle of more mature US FHIR Core profiles aligned with Release 4 and additional implementation guidance that explicitly specifies how to handle populations of patient data (batch exports) via FHIR to more efficiently enable population and learning health system-oriented services.

We seek comment on use cases where an API using FHIR Release 4 might support improved exchange between a provider and a registry. Specifically, we seek comment on how the use of this standard might:

- Reduce the burden of implementing multiple solutions for various types of exchange, while still supporting the variability needed to exchange information with registries devoted to the care of a population defined by a particular disease, condition, exposure, or therapy;
- Allow for the collection of detailed, standardized data on an ongoing basis for medical procedures, services, or therapies for particular diseases, conditions, or exposures;
- Support an overall approach to data quality, including the systematic collection of clinical and other health care data, using standardized data elements and procedures to verify the completeness and validity of those data;
- Improve and enhance the ability of providers to leverage feedback from a registry to improve patient care; and
- Address a sufficiently wide range of use cases to warrant the prioritization of technical innovation on API-based options over the continued development of use-case-specific solutions in future rulemaking.

We also welcome any other comments stakeholders may have on implementation of the registries provisions under section 4005 of the Cures Act.

X. Patient Matching Request for Information

Patient matching is a critical component to interoperability and the nation's health information technology infrastructure. Accurate patient matching helps health care providers access and share the right information on the right patient when and where it is needed.

Inaccurate patient matching can compromise safety, privacy, and lead to increased health care costs, as acknowledged in the Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriation Bill, 2017: [137]

> The Committee is aware that one of the most significant challenges inhibiting the safe and secure electronic exchange of health information is the lack of a consistent patient data matching strategy. With the passage of the HITECH Act, a clear mandate was placed on the Nation's healthcare community to adopt electronic health records and health exchange capability. Although the Committee continues to carry a prohibition against HHS using funds to promulgate or adopt any final standard providing for the assignment of a unique health identifier for an individual until such activity is authorized, the Committee notes that this limitation does not prohibit HHS from examining the issues around patient matching. Accordingly, the Committee encourages the Secretary, acting through the Office of the National Coordinator for Health Information Technology and CMS, to provide technical assistance to private-sector led initiatives to develop a coordinated national strategy that will promote patient safety by accurately identifying patients to their health information.

Similarly, the Fiscal Year 2018 Appropriations Bill [138] also included language regarding patient matching.

> The Committee is aware that a challenge inhibiting the safe and secure electronic exchange of health information is the lack of a consistent approach to matching patient data. The Committee encourages ONC to engage with stakeholders on private-sector led initiatives to develop a coordinated strategy that will promote patient safety by accurately identifying patients to their health information.

Section 4007 of the 21st Century Cures Act (Pub. L. 114–255) directs the Government Accountability Office (GAO) to conduct a study on patient matching. Specifically, the GAO was charged to review the policies and activities of the Office of the National Coordinator for Health Information Technology (ONC) and other relevant stakeholders, including standards development organizations, developers, providers, suppliers, payers, quality organizations, States, health information technology policy and technical experts, and other appropriate entities. The GAO report, *Approaches and Challenges to Electronically Matching Patients' Records across Providers,* was released in January 2019.[139] In this report, GAO describes (1) stakeholders' patient record matching approaches and related challenges; and (2) efforts to improve patient record matching identified by stakeholders. Stakeholders said more could be done to improve patient record matching, and identified several efforts that could improve matching. For example, some said that implementing common standards for recording demographic data; sharing best practices and other resources; and developing a public-private collaboration effort could each improve matching. Stakeholders' views varied on the roles ONC and others should play in these efforts and the extent to which the efforts would improve matching. Multiple stakeholders emphasized that no single effort would solve the challenge of patient record matching.

Patient matching may be defined as the linking of one patient's data within and across health care providers in order to obtain a comprehensive and longitudinal view of that patient's health care. At a minimum, this is accomplished by linking multiple demographic data fields such as name, birth date, sex, phone number, and

[137] *https://www.congress.gov/114/crpt/hrpt699/CRPT-114hrpt699.pdf.*

[138] *https://appropriations.house.gov/uploadedfiles/23920.pdf.*

[139] U.S. Government Accountability Office, *Approaches and Challenges to Electronically Matching Patients' Records across Providers,* GAO–19–197, *https://www.gao.gov/assets/700/696426.pdf.*

address. For this reason, accurate and standardized data capture and exchange and optimized algorithm performance are critical components to the accurate patient matching. With this in mind, ONC has taken several steps to better understand the patient matching landscape and to identify areas where ONC can assist in standards and technical development, coordination, and innovation. For example, in 2017, ONC launched the Patient Matching Algorithm Challenge, where six winners were awarded total prize winnings of $75,000.[140] The goals of this challenge were to bring about greater transparency and data on the performance of existing patient matching algorithms, spur the adoption of performance metrics for patient matching algorithm developers, and positively impact other aspects of patient matching such as deduplication and linking. In addition, in 2018, ONC showcased innovative technical and non-technical approaches to matching through hosting a patient matching track at ONC's Second Interoperability Forum.[141]

In this Request for Information (RFI), we seek comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. ONC and CMS collaborated to jointly issue complementary requests for information regarding patient matching. ONC is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability. Inaccurate patient matching can lead to inappropriate and unnecessary care; unnecessary burden on both patients and providers to correct misidentification, time consuming and expensive burden on health systems to detect and reconcile duplicate patient records and improper record merges; and poor oversite into fraud and abuse. Per a survey by the College of Healthcare Information Management Executives, one in five providers named lack of an appropriate patient matching strategy as the primary reason for inadvertent illness or injury.[142] We consider this a quality of care and patient safety issue and seek stakeholder input on creative, innovative, and effective approaches to patient matching within and across providers. We also intend to review the responses to this RFI in concert with the GAO report once published.

We specifically seek input on the following:

- It is a common misconception that technology alone can solve the problem of poor data quality, but even the most advanced, innovative technical approaches are unable to overcome data quality issues. Thus, we seek input on the potential effect that data collection standards may have on the quality of health data that is captured and stored and the impact that such standards may have on accurate patient matching. We also seek input on other solutions that may increase the likelihood of accurate data capture, including the implementation of technology that supports the verification and authentication of certain demographic data elements such as mailing address, as well as other efforts that support ongoing data quality improvement efforts.
- In concert with the GAO study referenced above, we seek input on what additional data elements could be defined to assist in patient matching as well as input on a required minimum set of elements that need to be collected and exchanged. We encourage stakeholders to review the Patient Demographic Record Matching section of the Interoperability Standards Advisory [143] and comment on the standards and implementation specifications outlined. Public comments and subject matter feedback on all sections of the Interoperability Standards Advisory are accepted year round.
- Also in alignment with the GAO study, we seek input on whether and what requirements for electronic health records could be established to assure data used for patient matching is collected accurately and completely for every patient. For instance, the adopted 2015 Edition ''transitions of care'' certification criterion (§ 170.315(b)(1)) currently includes patient matching requirements for first name, last name, previous name, middle name, suffix, date of birth, address, phone number, and sex. These requirement also include format constraints for some of the data.
- There are unique matching issues related to pediatrics and we seek comment on innovative and effective technical or non-technical approaches that could support accurate pediatric record matching.
- Recent research suggests that involving patients in patient matching may be a viable and effective solution to increase the accuracy of matching, and giving patients access to their own clinical information empowers engagements and improved health outcomes. We seek comment on potential solutions that include patients through a variety of methods and technical platforms in the capture, update and maintenance of their own demographic and health data, including privacy criteria and the role of providers as educators and advocates.
- In addition, we seek input on standardized metrics for the performance evaluation of available patient matching algorithms. Health IT developers are each relying on a number of patient matching algorithms, however, without the adoption of agreed upon metrics for the evaluation of algorithm performance across the industry, existing matching approaches cannot be accurately evaluated or compared across systems or over time.
- At the same time, we seek input on transparent patient matching indicators such as database duplicate rate, duplicate creation rate, and true match rate, for example, that are necessary for assessment and reporting. The current lack of consensus, adoption, and transparency of such indicators makes communication, reporting, and cross-provider or cross-organizational comparisons impossible, impedes a full and accurate assessment of the extent of the problem, prohibits informed decision making, limits research on complementary matching methods, and inhibits progress and innovation in this area.
- There are a number of emerging private-sector led approaches in patient matching that may prove to be effective, and we seek input on these approaches, in general. A number of matching services that leverage referential matching technology have emerged in the market recently, yet evaluations of this type of approach has either not been conducted or has not been made public. Other innovative technical approaches such as biometrics, machine learning and artificial intelligence, or locally developed unique identifier efforts, when used in combination with non-technical approaches such as patient engagement, supportive policies, data governance, and ongoing data quality improvement efforts may enhance capacity for matching.
- Finally, ONC seeks input on new data that could be added to the United States Core Data for Interoperability (USCDI) or further constrained within it in order to support patient matching.

[140] *https://www.hhs.gov/about/news/2017/11/08/hhs-names-patient-matching-algorithm-challenge-winners.html.*

[141] *https://www.healthit.gov/news/events/oncs-2nd-interoperability-forum.*

[142] *https://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf.*

[143] *https://www.healthit.gov/isa/patient-demographic-record-matching.*

XI. Incorporation by Reference

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies propose to incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(a)). Specifically, § 51.5(a) requires agencies to discuss, in the preamble of a proposed rule, the ways that the materials it proposes to incorporate by reference are reasonably available to interested parties or how it worked to make those materials reasonably available to interested parties; and summarize, in the preamble of the proposed rule, the material it proposes to incorporate by reference.

To make the materials we intend to incorporate by reference reasonably available, we provide a uniform resource locator (URL) for the standards and implementation specifications. In many cases, these standards and implementation specifications are directly accessible through the URLs provided. In instances where they are not directly available, we note the steps and requirements necessary to gain access to the standard or implementation specification. In most of these instances, access to the standard or implementation specification can be gained through no-cost (monetary) participation, subscription, or membership with the applicable standards developing organization (SDO) or custodial organization. In certain instances, where noted, access requires a fee or paid membership. As an alternative, a copy of the standards may be viewed for free at the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, 330 C Street SW, Washington, DC 20201. Please call (202) 690–7171 in advance to arrange inspection.

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. As discussed in section IV of this preamble, we have followed the NTTAA and OMB Circular A–119 in proposing standards and implementation specifications for adoption, including describing any exceptions in the proposed adoption of standards and implementation specifications. Over the years of adopting standards and implementation specifications for certification, we have worked with SDOs, such as HL7, to make the standards we propose to adopt, and subsequently adopt and incorporate by reference in the **Federal Register**, available to interested stakeholders. As described above, this includes making the standards and implementation specifications available through no-cost memberships and no-cost subscriptions.

As required by § 51.5(a), we provide summaries of the standards we propose to adopt and subsequently incorporate by reference in the Code of Federal Regulations. We also provide relevant information about these standards and implementation specifications throughout the preamble.

We have organized the following standards and implementation specifications that we propose to adopt through this rulemaking according to the sections of the Code of Federal Regulation (CFR) in which they would be codified and cross-referenced for associated certification criteria and requirements that we propose to adopt. We note, in certain instances, that we request comment in this proposed rule on multiple standards or implementation specifications that we are considering for adoption *and incorporation by reference* for particular use cases. We include all of these standards and implementation specifications in this section of the preamble.

Content Exchange Standards and Implementation Specifications for Exchanging Electronic Health Information—45 CFR 170.205

- CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting Implementation Guide for 2019, May 4, 2018

URL: https://ecqi.healthit.gov/system/files/QRDA_HQR_2019_CMS_IG_final_508.pdf.

This is a direct access link.

Summary: This guide is a CMS Quality Reporting Document Architecture Category I (QRDA I) implementation guide to the *HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture Category I, Release 1, STU Release 5 (published December 2017),* referred to as the HL7 QRDA I STU R5 in this guide. This guide describes additional conformance statements and constraints for EHR data submissions that are required for reporting information to the CMS for the Hospital Inpatient Quality Reporting Program 2019 Reporting Period. The purpose of this guide is to serve as a companion to the base HL7 QRDA I STU R5 for entities such as Eligible Hospitals (EH), Critical Access Hospitals (CAH), and vendors to submit QRDA I data for consumption by CMS systems including for Hospital Quality Reporting (HQR).

- CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2019, October 8, 2018

URL: https://ecqi.healthit.gov/system/files/2019_CMS_QRDA_III_Eligible_Clinicians_and_EP_IG-508.pdf.

This is a direct access link.

Summary: The Health Level Seven International (HL7) Quality Reporting Document Architecture (QRDA) defines constraints on the HL7 Clinical Document Architecture Release 2 (CDA R2). QRDA is a standard document format for the exchange of electronic clinical quality measure (eCQM) data. QRDA reports contain data extracted from electronic health records (EHRs) and other information technology systems. The reports are used for the exchange of eCQM data between systems for quality measurement and reporting programs. This QRDA guide contains the Centers for Medicare & Medicaid Services (CMS) supplemental implementation guide to the *HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture, Category III, STU Release 2.1 (June, 2017)* for the 2019 performance period. This HL7 base standard is referred to as the HL7 QRDA–III STU R2.1.

- Health Level 7 (HL7®) CDA R2 IG: C–CDA Templates for Clinical Notes R1 Companion Guide, Release 1 (C–CDA 2.1 Companion Guide), March 2017

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=447.

Access requires a ‘‘user account’’ and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Companion Guide to Consolidated Clinical Document Architecture (C–CDA) provides supplemental guidance to the Health Level Seven (HL7) CDA® R2 IG: C–CDA Templates for Clinical Notes STU Release 2.1 in support of the ONC 2015

Edition Health IT Certification Criteria (2015 Edition) Certified Electronic Health Record Technology requirements. This guide provides additional technical clarification and practical guidance to assist implementers to support best practice implementations of the 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification.

- Health Level 7(HL7®) CDA R2 Implementation Guide: C–CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1–US Realm

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=486.

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Implementation Guide contains guidance, supporting material and new templates to implement support for Unique Device Identifiers (UDIs) for implantable medical devices. The IG identifies changes needed to the C–CDA to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. The UDI components include the Device Identifier (DI) and the following individual production identifiers (PI): The lot or batch number, serial number, manufacturing date, expiration date, and distinct identification code.

- National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 (Approval Date for ANSI: July 28, 2017)

URL: http://www.ncpdp.org/Standards/Standards-Info.

Access requires registration, membership fee, a user account, and license agreement to obtain a copy of the standard.

Summary: SCRIPT standards are developed for transmitting prescription information electronically between prescribers, pharmacies, payers, and other entities for new prescriptions, changes of prescriptions, prescription refill requests, prescription fill status notifications, cancellation notifications, relaying of medication history, transactions for long-term care, electronic prior authorization and other transactions. New transactions in this update include Prescription drug administration message, New prescription requests, New prescription response denials, Prescription transfer message, Prescription fill indicator change, Prescription recertification, Risk Evaluation and Mitigation Strategy (REMS) initiation request, REMS initiation response, REMS request, and REMS response.

United States Core Data for Interoperability—45 CFR 170.213

- The United States Core Data for Interoperability (USCDI), Version 1 (v1)

URL: https://www.healthit.gov/USCDI.

This is a direct access link.

Summary: The United States Core Data for Interoperability (USCDI) establishes a minimum set of data classes that are required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time. Data classes listed in the USCDI are represented in a technically agnostic manner.

Application Programming Interface Standards—45 CFR 170.215

- HL7® FHIR® Foundation, Argonaut Data Query Implementation Guide Server, Version 1.0.2, December 15, 2016

URL: http://www.fhir.org/guides/argonaut/r2/Conformance-server.html.

This is a direct access link.

Summary: This profile defines the expected capabilities of an Argonaut Data Query server when conforming to the Argonaut Data Query IG. The conformance resource includes the complete list of actual profiles, RESTful operations, and search parameters supported by Argonaut Data Query Servers. Servers have the option of choosing from this list to access necessary data based on their local use cases and other contextual requirements.

- HL7® FHIR® Foundation, Argonaut Data Query Implementation Guide, Version 1.0.0, December 23, 2016

URL: http://www.fhir.org/guides/argonaut/r2/.

This is a direct access link.

Summary: The Argonaut Data Query Implementation Guide is based upon the core FHIR DSTU Release 2.0 API and documents security and authorization, data element query of the ONC Common Clinical Data Set, and document query of static documents. This specification describes four use cases and sets search expectations for each. Argonaut uses the SMART Guide for apps that connect to EHR data.

- Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) Release 2.0 Draft Standard for Trial Use (DSTU), Version 1.0.2–7202, October 24, 2015

URL: http://hl7.org/fhir/DSTU2/index.html.

This is a direct access link.

Summary: The Fast Healthcare Interoperability Resources (FHIR) Draft Standard for Trial Use (DSTU) Release 2.0, Version 1.0.2 is designed to enable information exchange to support the provision of health care in a wide variety of settings. The specification builds on and adapts modern, widely used, RESTful practices to enable the provision of integrated health care across a wide range of teams and organizations. HL7 FHIR solutions are built from a set of modular components called ''Resources''. These Resources can easily be assembled into working systems that solve real world clinical and administrative problems at a fraction of the price of existing alternatives. HL7 FHIR is suitable for use in a wide variety of contexts (*e.g.,* mobile phone apps, cloud communications, EHR-based data sharing, and server communication in large institutional health care providers). All resources have the following features in common: A URL that identifies it; common metadata; a human-readable XHTML summary; a set of defined common data elements; and an extensibility framework to support variation in health care.

- Health Level 7 (HL7®) Version 3.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 3 Standard for Trial Use (STU), April 19, 2017

URL: http://hl7.org/fhir/STU3/index.html.

This is a direct access link.

Summary: The Fast Healthcare Interoperability Resources (FHIR®) Standard for Trial Use (STU) Release 3 leverages the latest web standards and applies a tight focus on implementation. FHIR solutions are built from a set of modular components called ''Resources''. These resources can easily be assembled into working systems that solve real world clinical and administrative problems at a fraction of the price of existing alternatives. FHIR is suitable for use in a wide variety of contexts—mobile phone apps, cloud communications, EHR-based data sharing, server communication in large institutional health care providers, and much more. This third STU release includes a significant increase in the number of supported resources as well as revisions to previously published resources reflecting implementer feedback and increased maturity and stability.

- Health Level 7 (HL7®) Version 4.0.0 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, December 27, 2018

URL: http://hl7.org/fhir/R4/.
This is a direct access link.
Summary: The Fast Healthcare Interoperability Resources (FHIR®) Release 4 provides the first set of normative FHIR resources. This normative designation means that the future changes will be backward compatible for the first time. These resources define the content and structure of core health data which can be used by developers to build standardized applications. Release 4 provides new standard operation on how to obtain data from multiple patients via FHIR. API services that focus on multiple patients would enable health care providers to manage various internal patient populations as well as external services a health care provider may contract for to support quality improvement, population health management, and cost accountability vis-à-vis the provider's partners (*e.g.,* health plans).

- Health Level 7 (HL7®) Implementation Specification—FHIR Profile: Consent2Share FHIR Consent Profile Design, December 11, 2017

URL: https://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseView&release_id=1259.
The standard can be accessed through this link.
Summary: The Consent2Share FHIR Consent Profile Design provides instructions for using the FHIR ''Consent'' resource to capture a record of a health care consumer's privacy preferences. Implementing an instance of the FHIR Consent resource based on this guide allows for a patient consent to permit or deny identified recipient(s) or recipient role(s) to perform one or more actions regarding a patient's health information for specific purposes and periods of time.

- API Resource Collection in Health (ARCH) Version 1

URL: https://www.healthit.gov/ARCH.
This is a direct access link.
Summary: The API Resource Collection in Health (ARCH) is an implementation specification that list a set of base FHIR resources that Health IT Modules would need to support. The ARCH aligns with, and is directed by, the data policy specified in the US Core Data for Interoperability (USCDI) standard.

- SMART Application Launch Framework Implementation Guide Release 1.0.0, November 13, 2018

URL: http://hl7.org/fhir/smart-app-launch/.
This is a direct access link.
Summary: SMART on FHIR provides reliable, secure authorization for a variety of app architectures through the use of the OAuth 2.0 standard. This Authorization Guide supports the four uses cases defined for Phase 1 of the Argonaut Project. This profile is intended to be used by developers of apps that need to access FHIR resources by requesting access tokens from OAuth 2.0 compliant authorization servers. The profile defines a method through which an app requests authorization to access a FHIR resource, and then uses that authorization to retrieve the resource. Other Health Insurance Portability and Accountability Act (HIPAA)-mandated security mechanisms, such as end-user authentication, session time-out, security auditing, and accounting of disclosures, are outside the scope of this profile.

- IETF OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591), July 2015

URL: https://tools.ietf.org/html/rfc7591.
This is a direct access link.
Summary: This specification defines mechanisms for dynamically registering OAuth 2.0 clients with authorization servers. Registration requests send a set of desired client metadata values to the authorization server. The resulting registration responses return a client identifier to use at the authorization server and the client metadata values registered for the client. The client can then use this registration information to communicate with the authorization server using the OAuth 2.1 protocol. This specification also defines a set of common client metadata fields and values for clients to use during registration.

- OpenID Connect Core 1.0 Incorporating Errata Set 1, November 8, 2014

URL: http://openid.net/specs/openid-connect-core-1_0.html.
This is a direct access link.
Summary: OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. This specification defines the core OpenID Connect functionality: Authentication built on top of OAuth 2.0 and the use of Claims to communicate information about the End-User. It also describes the security and privacy considerations for using OpenID Connect.

XII. Response to Comments

Because of the large number of public comments normally received in response to **Federal Register** documents, we are not able to acknowledge or respond to them individually. We will consider all comments we receive by the date and time specified in the **DATES** section of this preamble, and, when we proceed with a subsequent document, we will respond to the comments in the preamble of that document.

We note that, throughout this proposed rule, we identified areas where we need more information before making a proposal (*i.e.,* requests for information). We note that comments we receive in response to these requests for information will not necessarily be addressed in the final rule, but will be used to inform future rulemaking.

XIII. Collection of Information Requirements

The Paperwork Reduction Act of 1995 (PRA) requires agencies to provide a 60-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to the Office of Management and Budget for review and approval. In order to fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;
2. The accuracy of the agency's estimate of the information collection burden;
3. The quality, utility, and clarity of the information to be collected; and
4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section. To comment on the collection of information or to obtain copies of the supporting statements and any related forms for the proposed paperwork collections referenced in this section, email your comment or request, including your address and phone number to *Sherrette.funn@hhs.gov,* or call the Reports Clearance Office at (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above email address within 60 days.

A. ONC–ACBs

We propose to add new ONC–ACB collection and reporting requirements for the certification of health IT to the 2015 Edition (and any subsequent edition certification) in § 170.523(p), (q), (t), and § 170.550(1).

As proposed for §§ 170.550(l), ONC–ACBs would not be able to certify health IT until they review and verify health IT developers' attestations confirming that the developers are compliant with Conditions and Maintenance of Certification requirements. ONC–ACBs would also submit the health IT developer attestations to ONC as proposed by § 170.523(q). We believe this will require minimal effort on behalf of ONC–ACBs as the ONC submission part will be electronically facilitated via the CHPL.

As proposed for § 170.523(p)(3), ONC–ACBs would be required to collect and report certain information to ONC related to real world testing plans and results. ONC–ACBs would be required to verify that the health IT developer submits an annual, publicly available real world testing plan and perform a completeness check for both real world testing plans and results. We believe ONC–ACBs will face minimum burden in complying with these new proposed requirements.

As proposed for § 170.523(t), ONC–ACBs would ensure health IT developers opting to take advantage of the Standard Version Advancement Process flexibility per § 170.405(b)(5) provide timely advance written notice to the ONC–ACB and all affected customers. ONC–ACBs would maintain a record of the date of issuance and the content of developers' notices, and timely post content of each notice received publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies. We believe this will require minimal effort on behalf of ONC–ACBs as the submission part will be electronically facilitated via the CHPL.

In the 2015 Edition proposed rule (80 FR 16894), we estimated fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements that applied to the ONC–AA and ONC–ACBs, including those previously approved by OMB. In the 2015 Edition final rule (80 FR 62733), we concluded that the regulatory ''collection of information'' requirements for the ONC–AA and the ONC–ACBs were not subject to the PRA under 5 CFR 1320.3(c). We continue to estimate less than ten annual respondents for all of the proposed regulatory ''collection of information'' requirements for ONC–ACBs under Part 170 of Title 45, including those previously approved by OMB and proposed in this proposed rule. Accordingly, the regulatory ''collection of information'' requirements under the Program described in this section are not subject to the PRA under 5 CFR 1320.3(c). We welcome comments on these conclusions and the supporting rationale on which they are based. For costs estimates of these proposed new regulatory requirements, we refer readers to section XIV. (*Regulatory Impact Analysis*) of this proposed rule.

B. Health IT Developers

We propose in 45 CFR 170.580(a)(2)(iii) that ONC may take action against a health IT developer for failure to comply with Conditions and Maintenance of Certification requirements. We proposed to generally use the same processes previously codified in regulation (§§ 170.580 and 170.581) to take administrative enforcement action. These processes would require health IT developers to submit information to ONC to facilitate and conclude its review. The PRA, however, exempts these information collections. Specifically, 44 U.S.C. 3518(c)(1)(B)(ii) excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

We propose in 45 CFR 170.402(b)(1) that a health IT developer must, for a period of 10 years beginning from the date each of a developer's health IT is first certified under the ONC Health IT Certification Program, retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program. We believe it will take approximately two hours per week on average to comply with our proposed record retention requirement. We welcome comments if stakeholders believe more or less time should be included in our estimate.

TABLE 4—ESTIMATED ANNUALIZED TOTAL BURDEN HOURS FOR HEALTH IT DEVELOPERS TO COMPLY WITH RECORDS RETENTION REQUIREMENTS

Code of Federal regulations section	Number of health IT developers	Average burden hours	Total
45 CFR 170.402(b)(1)	458	104	47,632
Total Burden Hours			47,632

XIV. Regulatory Impact Analysis

A. Statement of Need

This proposed rule is necessary to meet our statutory responsibilities under the 21st Century Cures Act (Cures Act) and to advance HHS policy goals to promote interoperability and mitigate burden for stakeholders. Proposals that could result in monetary costs for stakeholders include the: (1) Proposals to update the 2015 Edition health IT certification criteria; (2) proposals related to Conditions and Maintenance of Certification for a health IT developer; (3) proposals related to oversight for the Conditions and Maintenance of Certification; and (4) proposals related to information blocking.

While much of the costs of this proposed rule will fall on health IT developers that seek to certify health IT under the ONC Health IT Certification Program (Program), we believe the implementation and use of health IT certified to the 2015 Edition (including the new criteria in this proposed rule), compliance with the Conditions and Maintenance of Certification, and the limited exceptions to information blocking proposed would ultimately result in significant benefits for health care providers and patients. We outline some of these benefits below. We emphasize in this regulatory impact analysis (RIA) that we believe this proposed rule would create opportunities for new market entrants and would remove barriers to interoperability and electronic health information exchange, which would greatly benefit health care providers and patients.

We note in this RIA that there were instances in which we had difficulty quantifying certain benefits due to a lack of applicable studies and/or data. However, in such instances, we highlight the significant qualitative benefits of our proposals to advance an interoperable health system that empowers individuals to use their electronic health information (EHI) to the fullest extent and enables health care providers and communities to deliver smarter, safer, and more efficient care.

B. Alternatives Considered

We assessed whether there are alternatives to our proposals, specifically our proposals concerning EHI export, application programming interfaces (APIs), and real world testing. We have been unable to identify alternatives that would appropriately implement our responsibilities under the Cures Act and support interoperability. We believe our proposals take the necessary steps to fulfill the mandates specified in the Public Health Service Act (PHSA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Cures Act, in the least burdensome way. We are, however, open to less burdensome alternatives that meet statutory requirements and our goals. Accordingly, we welcome comments on our assessment and any alternatives we should consider.

C. Overall Impact

We have examined the impact of this proposed rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), Executive Order 13771 on Reducing Regulation and Controlling Regulatory Costs, the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), and Executive Order 13132 on Federalism (August 4, 1999).

1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis

Executive Orders 12866 on Regulatory Planning and Review and 13563 on Improving Regulation and Regulatory Review direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). OMB has determined that this proposed rule is an economically significant rule as the potential costs associated with this proposed rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this proposed rule.

2. Executive Order 13771—Reducing Regulation and Controlling Regulatory Costs

Executive Order 13771 on Reducing Regulation and Controlling Regulatory Costs was issued on January 30, 2017 and directs agencies to repeal two existing regulations for each new regulation issued in fiscal year (FY) 2017 and thereafter. It further directs agencies, via guidance issued by the Office of Management and Budget (OMB), that the total incremental costs of all regulations should be no greater than zero in FY 2018. The analysis required by Executive Order 13771, as supplemented by Executive Order 13777, adds additional requirements for analysis of regulatory actions. The new requirements under Executive Orders 13771 and 13777 do not change or reduce existing requirements under Executive Orders 12866 or 13563.

a. Costs and Benefits

We have estimated the potential monetary costs and benefits of this proposed rule for health IT developers, health care providers, patients, ONC-Authorized Certification Bodies (ONC–ACBs), ONC-Authorized Testing Laboratories (ONC–ATLs), and the federal government (*i.e.,* ONC), and have broken those costs and benefits out into the following categories: (1) Deregulatory actions (no associated costs); (2) updates the 2015 Edition Health IT certification criteria; (3) Conditions and Maintenance of Certification for a health IT developer; (4) oversight for the Conditions and Maintenance of Certification; and (5) information blocking.

In accordance with Executive Order 12866, we have included the RIA summary table as Table 25. In addition, we have included a summary to meet the regulatory reform analysis requirements under Executive Order 13771.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2016 dollars as it is the most recent data available to address all cost and benefit estimates consistently. We also note that estimates presented in the following ‘‘Employee Assumptions and Hourly Wage,’’ ‘‘Quantifying the Estimated Number of Health IT Developers and Products,’’ and ‘‘Number of End Users that Might Be Impacted by ONC’s Proposed Regulations’’ sections are used throughout this RIA.

For proposals where research supported direct estimates of impact, we estimated the benefits. For proposals where no such research was identified to be available, we developed estimates based on a reasonable proxy.

We note that interoperability can positively impact patient safety, care coordination, and improve health care processes and health outcomes.[144] However, achieving interoperability is a function of a number of factors including the capability of the technology used by health care providers. Therefore, to assess the benefits of our proposals, we must first consider how to assess their respective effects on interoperability holding other factors constant.

For the purpose of this analysis, we used regression analysis to calculate the impact of our real world testing and API proposals on interoperability. We assumed that the real world testing and API proposals would collectively have the same impact on interoperability as health IT certified to the 2014 Edition. Therefore, we estimated linear probability models that identified the impact of 2014 Edition certified health IT on hospitals’ interoperability.[145] We used data from the 2014 and 2015 American Hospital Association (AHA) Annual Survey Information Technology Supplement (IT Supplement), which consists of an analytic sample of 4,866 observations of non-federal acute care

[144] *https://www.qualityforum.org/Publications/2017/09/Interoperability_2016-2017_Final_Report.aspx.*

[145] The interoperability dependent variable is a binary indicator for whether a hospital routinely sends, receives, and integrates summary of care records electronically outside of its system and finds any health information electronically outside of its system.

hospitals that responded to the IT Supplement.[146] We controlled for additional factors such as participation in a health information exchange organization, hospital characteristics, and urban/rural status. More specifically, we used the following explanatory variables:

Edition = 1 if a hospital adopted 2014 Edition EHR, 0 otherwise
RHIO = 1 if a hospital participates in health information exchange organization, 0 otherwise
Government = 1 if a hospital is publically owned, 0 otherwise
Alt_teaching = 1 if a hospital is teaching, 0 otherwise
Nonprofit = 1 if a hospital is not for profit, 0 otherwise
Largebed = 1 if a hospital has more than 399 beds, 0 otherwise
Medbed = 1 if a hospital's number of beds is between 100 and 399, 0 otherwise
Urban_rural = 1 if a hospital is urban, 0 otherwise
CAH = 1 if a hospital is critical access, 0 otherwise
Year = year of the data (2014 and 2015)
S = state fixed effects

We found a statistically significant marginal effect of using 2014 Edition certified health IT associated with a five percentage point increase in interoperability.[147]

While we acknowledge that there might be shared benefits across proposals, we have taken steps to ensure that the benefits attributed to each proposal is unique to the proposal referenced. We assumed that this marginal effect is true for our proposals and distributed the 5% benefit across our real world testing and API proposals at (.1–1%) to (1–4%) respectively. Moreover, the number of providers impacted is proposal specific. Given data limitations, we believe this approach allows us to estimate the benefits of our proposals without double counting the impact each proposal might have on interoperability.

Employee Assumptions and Hourly Wage

We have made employee assumptions about the level of expertise needed to complete the proposed requirements in this section. For wage calculations for federal employees and ONC–ACBs, we have correlated the employee's expertise with the corresponding grade and step of an employee classified under the General Schedule (GS) Federal Salary Classification, relying on the associated employee hourly rates for the Washington, DC locality pay area as published by the Office of Personnel Management for 2016.[148] We have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages. Therefore, we have doubled the employee's hourly wage to account for overhead costs. We have concluded that a 100% expenditure on benefits is an appropriate estimate based on research conducted by HHS.[149]

We have used Bureau of Labor Statistics (BLS) data to calculate private sector employee wage estimates (*e.g.,* health IT developers, health care providers, HINs, attorneys, etc.), as we believe BLS provides the most accurate and comprehensive wage data for private sector positions. Just as with the General Schedule Federal Salary Classification calculations, we have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages.

All wage estimates (GS and BLS) have been calculated in 2016 dollars because OMB requested that agencies generate cost and benefit estimates in 2016 dollars under Executive Order 13771. If we were to represent wage estimates in 2017 dollars, then costs and benefits, including net benefits, would increase by 4%. For our final rule, we will consider using 2017 and even 2018 dollars, if available, for our cost and benefit estimates.

We welcome comments on our methodology for estimating labor costs.

Quantifying the Estimated Number of Health IT Developers and Products

In this section, we describe the methodology used to assess the potential impact of new 2015 Edition certification criteria on the availability of certified products in the health IT market. This analysis is based on the number of certified health IT products (*i.e.,* Health IT Modules), product capability, and the number of health IT developers that left, merged, and/or entered the health IT market between the establishment of the Program and implementation of the 2011 Edition and the implementation of the 2014 Edition.[150]

Market consolidation may occur as a result of a natural evolvement of a new industry.[151] We account for this factor in our analysis. In Table 5 below, we quantify the extent to which the certified health IT market consolidated between the 2011 Edition and 2014 Edition. We found that the number of health IT developers certifying products between the 2011 Edition and 2014 Edition decreased by 22.1% and the number of products available decreased by 23.2%.

TABLE 5—CERTIFIED HEALTH IT MARKET CONSOLIDATION FROM THE 2011 EDITION TO THE 2014 EDITION [a]

	2011 Edition	2014 Edition	Market consolidation (%)
Health IT Developers	1,017	792	−22.1
Products	1,408	1,081	−23.2

[a] For the purposes of these market consolidation calculations, we included the total number of active or suspended health IT products and their developers. Withdrawn products and their developers were excluded from this total.

Not all products are certified to all of the edition's certification criteria available in the Program. Modular certification allows a health IT developer to present a product for certification to a narrower scope of

[146] American Hospital Association Health IT Supplement Survey, *http://www.ahadata.com/aha-healthcare-database/.*

[147] Results were similar when we used logit or Probit specifications.

[148] *https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2016/DCB_h.pdf.*

[149] *See* U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation (ASPE), *Guidelines for Regulatory Impact Analysis,* at 28–30 (2016), *available at https://aspe.hhs.gov/system/files/pdf/242926/HHS_RIAGuidance.pdf.*

[150] Availability of 2014 CEHRT for Meaningful Users Providers, Health IT Policy Committee Data Update (Sept. 9, 2015), *available at http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Data_Update_Presentation_Final_2015-09-09.pdf.*

[151] *See* Graeme K. Deans, Fritz Kroeger, and Stefan Zeisel, The Consolidation Curve (Dec. 2002); J. David Cummins and Maria Rubio-Misas, *Deregulation, Consolidation, and Efficiency: Evidence from the Spanish Insurance Industry,* Journal of Money, Credit and Banking, Vol. 38, No. 2 (Mar. 2006), at 323–55; Martin Gaynor and Deborah Haas-Wilson, *Change, Consolidation, and Competition in Health Care Markets,* The Journal of Economic Perspectives, Vol. 13, No. 1 (Winter 1999), at 141–64.

specific use cases, which may be impacted at differing levels or may not be impacted by the proposals in this proposed rule. Therefore, we have estimated the number of 2015 Edition certified health IT products and health IT developers impacted by each proposal using proxies from historical data. Using the rates identified in Table 5, we then applied our estimate for market consolidation to estimate the number 2015 Edition certified health IT products and health IT developers that would be impacted by our policies in this proposed rule. Specifically, to estimate the number of 2015 Edition products and health IT developers in the market, we have assumed:

1. *Products capable of recording EHI will include new certification criteria.* We assume that products capable of recording patient health data will be the types of products most likely to be impacted by and include the new proposed certification criteria.

2. *Products capable of recording EHI data available in 2015 equal the number of products available in 2014.* In 2014, there were 710 products by 588 developers capable of recording EHI. Since the new criteria involve the access to and movement and exchange of EHI, we used only products that record EHI as a basis for our estimates. We believe the 2014 totals reflect a realistic estimate of the currently available products and their developers that could include the new 2015 certification criteria.

3. *Market consolidation rates denoted in Table 5 hold constant.* We assume that the rate of market consolidation for products (−23.2%) and health IT developers (−22.1%) from the 2011 Edition to the 2014 Edition holds constant for the 2015 Edition.

As shown in Table 6 below, based on the assumptions 1–3 above, we have estimated the total number of 2015 products (545) and their developers (458).

TABLE 6—TOTAL NUMBER OF HEALTH IT DEVELOPERS AND PRODUCTS BY SCENARIO

Scenario	Number of health IT developers	Number of products
2015 Edition Projection—All Products	617	830
2015 Edition Projection—Products Capable of Recording EHI	458	545

Number of End Users That Might Be Impacted by ONC's Proposed Regulations

For the purpose of this analysis, the population of end users differs according to the regulatory action proposed. In many cases, the end user population impacted is the number of hospitals and health care providers that possess certified health IT. Due to data limitations, our analysis regarding the number of hospitals and health care providers impacted by the regulatory action is based on the number of hospitals and health care providers that have historically participated in the Centers for Medicare & Medicaid Services (CMS) EHR Incentive Programs. Although there are limitations to this approach, participants in the CMS EHR Incentive Programs represent an adequate sample on which to base our estimates.[152] We estimate 439,187 health care providers [153] in 95,470 clinical practices [154] and 4,519 hospitals [155] will be impacted.

(1) Deregulatory Actions

Costs

We do not expect costs to be associated with the deregulatory action proposals.

Benefits

We expect the proposals for deregulatory actions to result in significant benefits for health IT developers, providers, ONC–ACBs, ONC–ATLs, and ONC. These expected benefits are detailed below.

1.1 Removal of the Randomized Surveillance Minimum Threshold Requirements

We have proposed to revise § 170.556(c) by revising the requirement that ONC–ACBs *must* conduct in-the-field, randomized surveillance and in its place specify that ONC–ACBs *may* conduct in-the-field, randomized surveillance. We have further proposed to remove § 170.556(c)(2), which specifies that ONC–ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year. We have also proposed to remove the requirement that ONC–ACBs make a good faith effort to complete randomized surveillance and the circumstances permitted for exclusion from this requirement found in § 170.556(c)(5).

These proposals would reduce burden on health care providers by reducing their exposure to randomized in-the-field surveillance of their health IT products. Health care providers expressed concern about the time commitment to support ONC–ACB randomized surveillance of health IT products, particularly if no non-conformities with certified health IT were found. Providers have generally stated that reactive surveillance (*e.g.,* complaint-based surveillance) is a more logical and economical approach to surveillance of health IT products implemented in a health care setting. The proposal in this proposed rule would provide health IT developers more time to focus on interoperability. It would also provide ONC–ACBs more time to respond to reactive surveillance, including health care provider complaints about certified health IT. In the 2015 Edition final rule, we did not independently estimate the costs for randomized surveillance. Rather, we relied on prior regulatory cost estimates for all surveillance actions. One of our ONC–ACBs charges a $3,000 annual fee per product for surveillance due to the new randomized surveillance requirements and to help normalize their revenue stream during down cycles between certification editions. Using this fee as a cost basis and

[152] *See* Office of the National Coordinator for Health Information Technology, *Office-based Health Care Professionals Participating in the CMS EHR Incentive Programs* (Aug. 2017), *dashboard.healthit.gov/quickstats/pages/FIG-Health-Care-Professionals-EHR-Incentive-Programs.php;* Office of the National Coordinator for Health Information Technology, *Hospitals Participating in the CMS EHR Incentive Programs* (Aug. 2017), *dashboard.healthit.gov/quickstats/pages/FIG-Hospitals-EHR-Incentive-Programs.php.*

[153] This estimate is the total number of eligible providers that ever participated in the CMS Medicare and Medicaid Electronic Health Record Incentive Program.

[154] This number was estimated based on the de-duplicated number of practices that had at least one clinician participate in the CMS Medicare Electronic Health Record Incentive Program.

[155] This estimate is the total number of eligible hospitals that ever participated in the CMS Medicare Electronic Health Record Incentive Program.

assuming it would apply to all certified health IT (as opposed to the market-adjusted universe of health IT that is used in other calculations in this RIA), we estimate that our proposal to remove the randomized surveillance ''2% minimum threshold'' requirements would result in cost savings between $6.8 and $13.7 million for all stakeholders. To arrive at this estimate, we multiplied the $3,000 annual fee per product for surveillance by the total number of products certified to the 2014 Edition which was 4,559 products at the time ($3,000 * 4,559 = $13.7 million). We anticipate the number of products certified for 2014 to decrease to a little as half of the original count over time. Therefore, we estimated the low end to be half of the $13.7 million (.5 * $13.7 million = $6.8 million). This estimate is based on feedback we received from our ONC–ATL and ONC–ACB stakeholders. ONC–ACBs performed randomized surveillance an average of 22 times the first year the requirement was in effect. The following year surveillance was performed an average of 2 times. We cannot predict how many randomized surveillance events the ONC–ACBs will perform now that we are not enforcing the requirement. It will be completely at the discretion of the ONC–ACBs.

We note that we considered other potential benefits that we were unable to quantify. We considered that health care provider burden may decrease from the elimination of the 2% minimum threshold requirements because a provider would previously aid the ONC–ACB in software demonstrations. However, we acknowledge that in the long term and moving forward, providers will likely be the party reporting more of the complaints that could result in reactive surveillance. We also considered that an additional benefit of the proposal would be reduced burden on ONC–ACBs. Feedback from ONC–ACBs indicates that having to meet a set number of surveillance activities in 12 months can be quite burdensome, especially when factoring in the active engagement necessary from provider participants. Last, we considered the potential benefit to health IT developers in having more surveillance focused on situations dealing with actual end-user concerns and/or difficulties. Health IT developers have indicated that they benefit from such surveillance, as feedback about conformance and capability can improve their products.

We welcome comments on potential means, methods, and relevant comparative studies and data that we could use to better quantify these benefits.

1.2 Removal of the 2014 Edition From the Code of Federal Regulations

We have proposed to remove the 2014 Edition certification criteria from the Code of Federal Regulations, which would directly benefit health IT developers, ONC–ACBs, ONC–ATLs, and ONC and indirectly benefit health care providers. When looking at the cost savings for removing the 2014 Edition certification criteria, we considered the current costs for maintaining those certifications and their surveillance (reactive), as well as the maintenance and administrative costs associated with supporting customer use of certified health IT for CMS EHR Incentive Program participation. The estimates below consider ONC analysis of the financial sustainability of ONC–ACBs and reflect data from as late as 2015.

We estimate that health IT developers would realize monetary savings from no longer supporting the 2014 Edition certification criteria due to a reduction in activities related to maintaining certification and surveillance. We are aware that one of our ONC–ACBs charges an inherited certified status (ICS) fee of $1,000. This fee has been applied over the last calendar year. Over that time period, the number of new, unique 2014 Edition products has been declining (24 products in the last calendar year, and no new products in the last four months) compared to the number of ICS certifications (569). Just assuming the cost of continued ICS certification, health IT developers would be paying approximately $569,000 each year to keep their 2014 Edition products up-to-date.

We are not aware of comparable fees charged by ONC–ATLs; however, based on our experience with the Program, we expect health IT developers would realize similar cost savings associated with ONC–ATL maintenance of the testing component associated with ICS. Thus, we estimate an additional $569,000 cost savings for health IT developers due to the reduced testing requirements.

A recent study conducted by ONC indicates that 2014 Edition ICS certification is not profitable for ONC–ACBs, which is why one ONC–ACB charged an additional $3,000 annual fee per product for surveillance for 2015 Edition certifications. In 2015, the net income for ONC–ACBs dropped 99% from about $5,310,000 in 2014 to $67,000 due to a decline in revenue from a drop in new 2014 Edition certified health IT products without a significant drop in expenses. We do not have enough information to calculate what percentage of ONC–ACB expenses are the direct result of 2014 Edition certification maintenance; however, our research indicates that it is significantly less profitable for ONC–ACBs to maintain 2014 Edition certification criteria (*e.g.,* through ICS attestation and reactive surveillance) than to certify new 2014 Edition certified health IT products.

We also attempted to identify a potential reduction in maintenance and administrative costs as a result of removing 2014 Edition certification criteria. We could not obtain data to conduct a full quantitative analysis specific to the reduction of health IT developer and health care provider costs related to supporting and maintaining the 2014 Edition. We seek comment on methods to quantify potential costs for maintaining and supporting products to previous editions.

We did conduct a review of academic literature and qualitative analysis regarding potential savings from no longer supporting the 2014 Edition. We looked at data in IT industry systems as whole, which showed that upgrading outdated legacy systems saves resources otherwise spent on maintaining compatibilities to multiple systems and also increases quality and efficiency.[156] Furthermore, as technology evolves, newer software and products allow for smoother updates compared to their predecessors. Newer products provide better security features that are able to address both new and existing issues. In addition, older software has an increased risk of failure, which, in the health IT industry, increases risk to patient safety.

From the implementer's perspective, the research indicates that retaining legacy systems tends to inhibit scalability and growth for businesses. The perpetuity of outdated legacy systems increases connection and system integration costs and limits the ability to realize increased efficiency through IT implementation. Newer products are developed to current specifications and updated standards, which decreases barriers and marginal cost of ancillary product implementation and increases the accessibility of data in ancillary systems—including via mobile devices and the latest applications. Finally, office staff in a health care setting would no longer need to be trained to accommodate differing data access

[156] James Crotty and Ivan Horrocks, *Managing legacy system costs: A case study of a meta-assessment model to identify solutions in a large financial services company,* Applied Computing and Informatics (2017), at 1–9.

needs or workarounds required to integrate to the legacy product.[157]

The research also indicates that retaining legacy software would not be beneficial or profitable to the health IT market. Prolonging backwards compatibility of newer products to legacy systems encourages market fragmentation.[158] Limiting fragmentation encourages innovation and attracts more developers by reducing barriers and the marginal cost of development to multiple platforms. Health IT stakeholders have expressed that system fragmentation increases the cost to develop and maintain health IT connectivity for data exchange and to integrate software supporting administrative and clinical processes, as well as limiting the feasibility of developing products to support specialty clinical care. This direct feedback suggests that fragmentation is having a negative impact on the interoperability and usability of health IT systems for health care providers. We intend to encourage the health IT market to keep progressing with a baseline expectation of functionalities that evolve over time. This requires limiting fragmentation by no longer supporting outdated or obsolete legacy software.[159]

We also estimate that additional savings could be realized by reducing regulatory complexity and burden caused by having two certification editions. For example, in the 2015 Edition final rule, we added new requirements, such as disclosure and transparency requirements, that applied to all certified product editions. This required significant effort by health IT developers and ONC–ACBs to execute the requirements, and both groups found it challenging to complete the task in the original timeframe provided by ONC. We have observed that the task of managing two different editions within different rules increases complexity and burden for ONC staff, contractors, ONC–ACBs, CMS programs referencing the certification criteria, and other stakeholders, as compared to our proposal to remove the 2014 Edition certification criteria. However, we are unable to estimate these benefits because we have no means for quantifying the benefits gained from only using the 2015 Edition. We welcome comments on potential means, methods, and relevant comparative studies and data that we could use to quantify these benefits.

We also expect that health care providers would benefit from this proposal because such action would likely motivate health IT developers to certify health IT products to the 2015 Edition, thus enabling providers to use the most up-to-date and supported systems to care for patients. The 2015 Edition certification criteria facilitates greater interoperability for several clinical health information purposes and enables health information exchange, including APIs, through new and enhanced certification criteria, standards, and implementation specifications. The certification criteria also allow for updates to documents and data standards and focus on the establishment of an interoperable health information infrastructure. We welcome comments on potential means, methods, and relevant comparative studies and data that we could use to quantify these benefits.

1.3 Removal of the ONC-Approved Accreditor From the ONC Health IT Certification Program

We expect ONC to realize monetary cost savings from the proposal to remove the ONC- Approved Accreditor (ONC–AA) from the Program. We expect ONC to realize costs savings from no longer: (1) Developing and publishing a **Federal Register** Notice and listserv; (2) monitoring the open application period and reviewing and making decisions regarding applications; and (3) oversight and enforcement of the ONC–AA. We have calculated the estimated annual cost savings for this proposal, taking into consideration that the ONC–AA renewed its status every three years.

The ONC–AA's expertise is in the ISO/IEC 17065 standard. Therefore, to effectively collaborate with the ONC–AA for Program activities, ONC allocates resources for working with the ONC–AA and informing the ONC–AA of scheme requirements and applicable policy interpretations, which we have and can provide directly to the ONC–ACBs. The amount of ONC resources allocated depends on current Program activities and need. For our calculations, we used the estimated hours for collaborating with and informing an ONC–AA in 2017 (using 2016 wage estimates). We estimate that ONC spent approximately 110 hours collaborating with the ONC–AA in 2017, which includes (all at the GS–13, Step 1 level): Annual assessments; providing appropriate guidance; implementing new requirements and initiatives; and consultations as necessary. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate the annual cost savings to be $3,238.

We estimate that ONC would commit approximately eight hours of staff time to develop the **Federal Register** Notice, which would include approximately: Four hours for drafting and review by an analyst at the GS–13, Step 1 level; two hours for review and analysis by senior certification staff at the GS–14, Step 1 level; and two hours for review and submittal for publication by Immediate Office staff at the GS–15, Step 1 level. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. The hourly wage with benefits for a GS–14, Step 1 employee located in Washington, DC is approximately $104.34. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, we estimate the annual cost savings to be $269. Additionally, we estimate a cost of $477 to publish each page in the **Federal Register**, which includes operational costs. The **Federal Register** Notice for ONC–AAs requires, on average, one page in the **Federal Register** (every three years), so we estimate an additional annual cost savings of $159.

We estimate that ONC would commit approximately two hours of staff time by an analyst at the GS–13, Step 1 level to draft, review, and publish the listserv to announce the **Federal Register** Notice. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate the annual cost savings to be $59.

We estimate that ONC would commit approximately 25 hours of staff time to manage the open application process, review applications and reach application decisions, which would include approximately: 20 hours by an analyst at the GS–13, Step 1 level; three hours by senior certification staff at the GS–14, Step 1 level; and two hours for review and approval by Immediate Office staff at the GS–15, Step 1 level. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. The hourly wage with benefits for a GS–14, Step 1 employee located in Washington, DC is approximately $104.34. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, we estimate the annual cost savings to be $775.

Taking all of these potential costs savings into consideration, we estimate

[157] *Id.*

[158] Il-Horn Hann, Byungwan Koh, and Marius F. Niculescu, *The Double-Edged Sword of Backward Compatibility: The Adoption of Multigenerational Platforms in the Presence of Intergenerational Services,* Inform. Systems Res. (2016), at 112–30.

[159] *Id.*

the overall annual costs savings for our proposal to remove the ONC–AA from the Program to be $4,500.

1.4 Removal of Certain 2015 Edition Certification Criteria

In section III.B.4 of this proposed rule, we propose to remove the following certification criteria from the 2015 Edition: § 170.315(b)(4) ''Common Clinical Data Set summary—create;'' (b)(5) ''Common Clinical Data Set summary—receive'', § 170.315(a)(10) ''Drug formulary and preferred drug list checks,'' § 170.315(a)(11) ''Smoking status,''§ 170.315(a)(13) ''Patient-specific education resources'' and § 170.315(e)(2) ''Secure messaging.''

For determining calculations for the majority of the proposed removal of certain 2015 Edition certification criteria, we used the assumptions below. For the proposed removal of § 170.315(b)(4) Common Clinical Data Set summary—create and (b)(5) Common Clinical Data Set summary—receive, we took a slightly different approach discussed in section 1.4.1.

In the 2015 Edition final rule, we estimated the costs for developing and preparing health IT to meet the 2015 Edition certification criteria. The development and preparation costs we estimated were derived through a health IT developer per criterion cost. We estimated the development and preparation costs over a four-year period and we projected the costs would be unevenly distributed. In figuring out the cost savings for the deregulatory actions, we initially used the distribution from the 2015 Edition, but then adjusted the percentages of development and preparation costs due to current empirical and anecdotal evidence. The distribution was reevaluated to account for 2019 and we estimate the actual development and preparation distribution for 2018 to be 35% and for 2019 to be 15%. We took the average development and preparation cost estimates (low and high) per criterion from Table 14 of the 2015 Edition final rule (80 FR 62737). We then used our new distribution to figure out the cost per year for years 2018 and 2019. We took the total estimated costs for 2018 and 2019 and divided that by 12 to determine the cost savings per month and took a range of 6–12 months.

To determine the testing costs of the deregulatory actions, we took the number of health IT developers who develop products for certification for the identified criteria from the 2015 Edition final rule and then figured out the average cost per criterion. Based on the costs that one of the ONC–ATLs charges for testing, we estimated the average cost for testing per criterion and determined subsequent cost savings. In 2017, only about five to ten percent of products have been tested and certified compared to the number of certified 2014 Edition products. Therefore, up to 90 to 95 percent of products remain to be tested and certified to the 2015 Edition.

We estimate the total cost savings by multiplying the number of health IT developers who developed products for certification to a certain criterion by the estimated cost per criterion, $475. We then took five percent of that number to figure out the high end for the cost savings. We then took 10 percent to figure out the low end. The five percent was derived from looking at the number of unique developers who have at least one active 2014 Edition product and the number of unique developers who have at least one active 2015 Edition. The denominator is the number of unique developers who have at least one active 2014 Edition product, which is 793. The numerator is the number of unique developers who have at least one active 2015 Edition product and one active 2014 edition product, which is 41. (41/793 = 0.0517024 or 5 percent).

1.4.1 Common Clinical Data Set Summary Record Criteria

We propose to remove the Common Clinical Data Set summary—create (§ 170.315(b)(4)) and Common Clinical Data Set summary—receive (§ 170.315(b)(5)) criteria.

We expect ONC to realize cost savings associated with internal infrastructure support and maintenance, which would include actions such as (1) developing and maintaining information regarding these criteria on the ONC website; (2) creating documents related to these criteria and making those documents 508 compliant; (3) updating, revising, and supporting Certification Companion Guides, test procedures, and test tools; and (4) responding to inquiries concerning these criteria. Based on ONC data on the number of inquiries received since early 2016, we estimate approximately 12 annual inquiries about § 170.315(b)(4) and (5) respectively (24 total inquiries for two criteria). We estimate it will take an analyst at the GS–13, Step 1 level an average of two hours to conduct all tasks associated with each inquiry. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate the annual cost savings to be $4,238.

We do not expect cost savings associated with software maintenance because both of these criteria incorporate the Common Clinical Data Set and essentially the same data input and validation requirements as the transitions of care criterion (§ 170.315(b)(1)). The removal of these two criteria would not affect the test data and software maintenance costs, as the same test data and software validation elements remain in § 170.315(b)(1) and the Common Clinical Data Set used in other criteria.

ONC–ACBs could realize minimal savings, as they would need to conduct slightly less surveillance based on the two products that are currently certified to these criteria. We expect these potential cost savings to be de minimis and have therefore not estimated them.

Taking all these potential costs savings into consideration, we estimate the overall annual costs savings for our proposal to remove the Common Clinical Data Set summary record certification criteria from the 2015 Edition to be $4,238. We welcome comments on the above estimates and methods we could use to better quantify these benefits.

1.4.2 Drug Formulary and Preferred Drug List Checks

We propose to remove the 2015 Edition ''drug formulary and preferred drug list checks'' criterion in § 170.315(a)(10)). To calculate the cost savings for removing this criterion, we used the 2015 Edition estimated costs for development and preparation for this criterion which were between $15,750 and $31,500. We believe that 35% of developers would be still newly certifying in 2018 and 15% in 2019 and applied the proportions respectively. We estimated the cost of development and preparation costs to be between $5,512.50 and $11,025 for 2018 and $2,362.50 and $4,725 for 2019. We calculated the cost per month for years 2018 and 2019 and using the high point estimates, estimated the development and preparation costs over a 6 to 12 month period between August 2018 to August 2019 to be between $4,068.75 and $6,825.

To calculate the cost for testing for this criterion, we multiplied the 5 developers that we estimated in the 2015 Edition to develop products to this criterion by our estimated cost to test per criterion of $475. The estimated cost per criterion was based on what one ONC–ATL charged for testing and averaged per criterion. To be conservative in our calculations, we reduced the number by 10% and 5% respectively resulting in $2,137.50 and $2,256.25.

Taking these estimated costs into account we expect cost savings to remove the 2015 Edition ‘‘drug formulary and preferred drug list checks’’ criterion to be between $8,962.50 and $9,081.25.

1.4.3 Smoking Status

We propose to remove the 2015 Edition ‘‘smoking status’’ criterion (§ 170.315(a)(11)), which would include removing it from the 2015 Edition Base EHR definition. To calculate the cost savings for removing this criterion, we used the 2015 Edition estimated costs of developing and preparing the criterion to the 2015 Edition, between $15,750 and $31,500 and estimated that 35% of developers would be newly certified in 2018 and 15% in 2019. We estimated the cost of development and preparation costs to be between $5,512.50 and $11,025 for 2018 and $2,362.50 and $4,725 for 2019. We calculated the cost per month for years 2018 and 2019 and using the high point estimates, estimated the development and preparation costs over a 6 to 12 month period between August 2018 and August 2019. We estimated the costs to be between $4,068.75 at 6 months and $6,825 at 12 months.

To calculate the cost for testing for this criterion, 5 developers were estimated in the 2015 Edition to develop products to this criterion. We multiplied the 5 developers by our estimated cost to test per criterion of $475. This estimated cost per criterion was based on what one ONC–ATL charged for testing and averaged per criterion. To be conservative, we reduced the number by 10% and 5% respectively resulting in $2,137.50 and $2,256.25.

Taking these estimated costs into account we expect cost savings to remove the 2015 Edition ‘‘smoking status’’ criterion to be between $8,962.50 and $9,081.25.

1.4.4 Patient-Specific Education Resources

We propose to remove the 2015 Edition ‘‘patient-specific education resources’’ certification criterion (§ 170.315(a)(13)). To estimate the cost of removing this criterion, we used the 2015 Edition estimated costs for development and preparation which is between $4,709,880 and $6,279,840. We believe that 35% of developers would be still newly certifying in 2018 and 15% in 2019 and applied the proportions respectively. We estimated the cost of development and preparation to be between $1,648,458 and $2,197,944 for 2018 and $706,482 and $941,976 for 2019. We calculated the cost per month for years 2018 and 2019 and using the high point estimates, estimated the development and preparation costs over a 6 to 12 month period, within August 2018 to August 2019. We estimated the costs to be between $850,395 at 6 months and $1,360,632 at 12 months. To calculate the testing cost for this criterion, we multiplied the estimates from the 2015 Edition of 249 developers that we estimated would develop products to this criterion by our estimated cost to test per criterion of $475. The estimated cost per criterion was based on what one ONC–ATL charged for testing and averaged per criterion. To be conservative, we reduced the number by 10% and 5% respectively resulting in $106,447.50 and $112,361.25. Taking these estimated costs into account, we expect the cost savings of removing the 2015 Edition ‘‘Patient-specific education resources’’ criterion to be between $1,467,079.50 and $1,472,993.25.

1.4.5 Secure Messaging

We propose to remove the 2015 Edition ‘‘secure messaging’’ criterion (§ 170.315(e)(2)). To estimate the cost savings of removing this criterion, we used the estimates from the 2015 Edition final rule for development and preparation costs which is between $1,552,320 and $3,104,640. We estimated that 35% of developers would be still newly certifying in 2018 and 15% in 2019 and applied the proportions respectively. We estimated the cost of development and preparation costs to be between $543,312 and $1,086,624 for 2018 and $232,848 and $465,696 for 2019. We then calculated the cost per month for years 2018 and 2019 and using the high point estimates, estimated the development and preparation costs over a 6 to 12 month period, between August 2018 to August 2019 to be between $401,016 at 6 months and $672,672 at 12 months. To calculate the cost for testing this criterion, we multiplied the 246 developers that we estimated in the 2015 Edition would develop products to this criterion by our estimated cost to test per criterion of $475. The estimated cost per criterion was based on what one ONC–ATL charged for testing and averaged per criterion. To be conservative, we reduced the number by 10% and 5%, respectively, resulting in $105,165 and $111,007.50. Taking these estimated costs into account, we estimate the cost savings of removing the 2015 Edition ‘‘Secure messaging’’ criterion to be between $777,837 and $783,678.50.

1.5 Removal of Certain Certification Requirements

We propose to remove § 170.523(k)(1)(iii)(B), which requires ONC–ACBs to ensure that certified health IT includes a detailed description of all known material information concerning limitations that a user may encounter in the course of implementing and using the certified health IT, whether to meet ‘‘meaningful use’’ objectives and measures or to achieve any other use within the scope of the health IT's certification. We also propose to remove § 170.523(k)(1)(iv)(B) and (C), which state that the types of information required to be disclosed include but are not limited to: (B) Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified; (C) Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

To calculate the savings related to removing these two disclosure requirements, we estimated 830 products certified to the 2015 Edition. We did so by applying the market consolidation rate of −23.2% which was the rate observed between 2011 and 2014 Editions. Assuming that an ONC–ACB spends 1 hour on average reviewing costs, limitations and mandatory disclosures, we estimate the time saved by no longer having to review the limitations to be two-thirds of an hour. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30 and we assume this to be the hourly rate for an ONC–ACB reviewer. We multiplied 830, the projected number of certified products, by two- thirds of an hour and the assumed hourly rate and calculated the cost savings to be $48,859.

(2) Updates to the 2015 Edition Certification Criteria

The following section details the costs and benefits for updates to the 2015 Edition health IT certification criteria, which includes (1) costs and benefits to update certain 2015 Edition criteria to due to the adoption of the United States Core Data for Interoperability (USCDI) as a standard and (2) costs for new 2015 Edition criteria for electronic health information export, API, privacy and security, and Data Segmentation for Privacy (DS4P)-Send and Data Segmentation for Privacy-Receive, and consent management for APIs.

2.1 United States Core Data for Interoperability

In order to advance interoperability by ensuring compliance with new structured data and code sets that support the data, we propose in this proposed rule to remove the ''Common Clinical Data Set'' definition and its references from the 2015 Edition and replace it with the ''United States Core Data for Interoperability'' (USCDI) standard, naming Version 1 (v1) in § 170.213 and incorporating it by reference in § 170.299. The USCDI v1 establishes a minimum set of data classes (including structured data) that are required for health IT to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time.

The USCDI v1 adds 2 new data classes, ''Clinical Notes'' and ''Provenance'' that were not defined in the CCDS, which will require updates to the Consolidated Clinical Document Architecture (C–CDA) standard and updates to the following certification criteria: § 170.315(b)(1) (transitions of care); (e)(1) (view, download, and transmit to 3rd party); (g)(6) (Consolidated CDA creation performance); (f)(5) (transmission to public health agencies—electronic case reporting); and (g)(9) (application access—all data request). From our analysis of the C–CDA standard, we conclude that the requirements of ''Provenance'' data class are already met by the existing C–CDA standard, and will not require any new development. Therefore, we have estimated the proposed cost to health IT developers to add support for ''Clinical Notes'' data class in C–CDA, and the necessary updates to the affected certification criteria. These estimates are detailed in Table 7 below and are based on the following assumptions:

1. *Health IT developers will use the same labor costs and data models.* Table 7 shows the estimated labor costs per product for a health IT developer to develop support for the additional USCDI data element in the C–CDA standard and affected certification criteria. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 7.

2. *A proxy is needed to project the number of 2015 Edition certified health IT products.* We estimate that 545 products from 458 developers will be affected by our proposal. Our proxy is based on the number of 2014 Edition certified health IT products that are capable of recording patient data.[160] There were 710 products by 588 developers with at least one 2014 Edition product capable of recording patient data. We then multiplied these numbers by our certified health IT market consolidation estimates of −22.1% and −23.2% to project the number of 2015 developers and products, respectively.

3. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $50.14.[161]

TABLE 7—COSTS TO HEALTH IT DEVELOPERS TO DEVELOP SUPPORT FOR THE ADDITIONAL USCDI DATA ELEMENT IN C–CDA STANDARD AND AFFECTED CERTIFICATION CRITERIA

[2016 Dollars]

Tasks	Details	Lower bound hours	Upper bound hours	Remarks
Update C–CDA creation)	New development to support "Clinical Notes" for C–CDA and C–CDA 2.1 Companion Guide.	800	1,800	(1) Lower bound assumes health IT already has developed C–CDA R2.1 into their system and only needs to be updated for new data class. (2) Upper bound estimates effort for organizations that are on older versions of C–CDA standard, for example C–CDA R1.1.
§ 170.315(b)(1) (transitions of care)	New development to support "Clinical Notes" for C–CDA and C–CDA 2.1Companion Guide.	200	600	Necessary updates to health IT to support the new data class to meet the criteria requirements.
§ 170.315(b)(6) (data export)	New development to support "Clinical Notes" for C–CDA and C–CDA 2.1 Companion Guide.	300	800	Necessary updates to health IT to support the new data class to meet the criteria requirements.
§ 170.315(e)(1) (view, download, and transmit to 3rd party).	New development to support "Clinical Notes" for C–CDA and C–CDA 2.1Companion Guide.	400	1,000	Necessary updates to health IT to support the new data class to meet the criteria requirements.
§ 170.315(g)(6) (Consolidated CDA creation performance).	New development to support "Clinical Notes" for C–CDA and C–CDA 2.1 Companion Guide.	200	600	170.315(b)(1) and § 170.315(g)(6) are related and may be developed together.
Total Hours		1,900	4,800	
Hourly Rate		$100.28		
Cost per Product		$190,532	$481,344	
Total Cost (545 products)		$103.8M	$262.3M	

[160] We defined ''products capable of recording patient data'' as any 2014 Edition health IT product that was certified for at least one of the following criteria: Demographics ((a)(5)), Medication List ((a)(7)), Medication Allergy List ((a)(8)), Problem List ((a)(6)), and Family Health History ((a)(12)).

[161] *https://www.bls.gov/oes/2016/may/oes439061.htm.*

We estimate that the cost to a health IT developer to develop support for the additional USCDI data element would range from $190,532 to $481,344. Therefore, assuming 545 products, we estimate that the total annual cost to all health IT developers would, on average, range from $103.8 million to $262.3 million. This would be a one-time cost to developers per product that is certified to the specified certification criteria and would not be perpetual.

We believe this proposal would benefit health care providers, patients, and the industry as a whole. Clinical notes and provenance were included in the draft USCDI v1 based on significant feedback from the industry, which highly regarded their desirability as part of interoperable exchanges. The free text portion of the clinical notes was most often relayed by clinicians as the data they sought, but were often missing during electronic health information exchange. Similarly, the provenance of data was also referenced by stakeholders as a fundamental need to improve the trustworthiness and reliability of the data being exchanged. We expect improvements to interoperable exchange of information and data provenance to significantly benefit providers and patients. However, we are not aware of an approach for quantifying these benefits and welcome comments on potential approaches to quantifying these benefits.

2.2 Electronic Health Information Export

We have proposed a new 2015 Edition certification criterion for ‘‘electronic health information export’’ in § 170.315(b)(10). The intent of this criterion is to provide patients and health IT users a means to efficiently export the entire electronic record for a single patient or all patients in a computable, electronic format. Further, it would facilitate the receiving health IT system’s interpretation and use of the EHI to the extent reasonably practicable using the health IT developer’s existing technology. This outcome would promote exchange, access, and use of electronic health information. It would also facilitate health care providers’ ability to switch health IT systems or migrate electronic health information for use in other technologies. This proposed criterion supports two specific use cases. First, it supports the export for a single patient that would need to be enabled upon valid request from a user or a patient. Second, the EHI export functionality for all patients’ data would support a health care provider or health system in switching health IT systems.

Costs

This section describes the estimated costs of the ‘‘electronic health information export’’ certification criterion. The cost estimates are based on the following assumptions:

1. *Health IT developers will use the same labor costs and data models.* Table 8 shows the estimated labor costs per product for a health IT developer to develop and maintain the electronic health information export functionality. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 8.

2. *A proxy is needed to project the number of 2015 Edition certified health IT products containing the ‘‘electronic health information export’’ certification criterion.* We estimate that 545 products from 458 developers will contain the ‘‘electronic health information export’’ criterion. To develop these estimates we first identified a proxy for the number of health IT developers that may create a 2015 Edition certified health IT product containing the ‘‘electronic health information export’’ criterion. Our proxy is based on the number of 2014 Edition certified health IT products that are capable of recording patient data.[162] We based our estimates on these products because data must be captured to be exported under the proposed criterion. There were 710 products by 588 developers with at least one 2014 Edition product capable of recording patient data. We then multiplied these numbers by our certified health IT market consolidation estimates of −22.1% and −23.2% to project the number of 2015 developers and products, respectively.

3. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a ‘‘Software Developer’’ is $50.14.[163]

TABLE 8—ESTIMATED LABOR COSTS TO DEVELOP AND MAINTAIN THE ELECTRONIC HEALTH INFORMATION EXPORT CRITERION PER PRODUCT

Activity	Lower bound hours	Upper bound hours	Remarks
Task 1: Developing the Data Dictionary and exporting the EHI in a developer format (per product).	160	1,600	This is the effort to document all the data exported by the product for a single patient and for all patients. The lower bound assumes that the health IT developer already has a standard format in which they are exporting the data for either case (*e.g.,* C–CDA for single patient, CSV file or database dump for all data) and the effort is merely to publish it to the users. On the other hand, the upper bound reflects the case where the health IT has to develop the export capability de novo into their product, and document the data output. This still assumes that the developer will be able to use the format of their choice. *Note: This is a one-time cost to develop the export capability.*
Task 2: Maintaining the Data Dictionary and performing export when requested (per product).	80	800	This is the annual maintenance cost charged by health IT developers to provide C–CDA feed to providers. This is a yearly update to products that are typically modest. The lower bound estimate assumes the effort when there are only minor changes to the product. The upper bound estimate assumes the effort when the product supports a substantial number of new data classes.

[162] We defined ‘‘products capable of recording patient data’’ as any 2014 Edition product that was certified for at least one of the following criteria: Demographics ((a)(5)), Medication List ((a)(7)), Medication Allergy List ((a)(8)), Problem List ((a)(6)), and Family Health History ((a)(12)).

[163] *https://www.bls.gov/oes/2016/may/oes439061.htm.*

TABLE 8—ESTIMATED LABOR COSTS TO DEVELOP AND MAINTAIN THE ELECTRONIC HEALTH INFORMATION EXPORT CRITERION PER PRODUCT—Continued

Activity	Lower bound hours	Upper bound hours	Remarks
Task 3: Maintaining the software to perform the electronic health information export (per product).	80	800	This is the annual cost to update the software that would generate the data access files. The lower bound estimates the cost to maintain the software when there are minor changes to the product, including updates to underlying software (*e.g.,* database versions, operating systems, etc.). The upper bound estimate accounts for substantial reworking of the export software program to support new data classes or new data formats.
Total Labor Hours	320	3,200	

TABLE 9—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO HEALTH IT DEVELOPERS TO PERFORM TASK 1 FOR THE ELECTRONIC HEALTH INFORMATION EXPORT CRITERION

[2016 Dollars]

	Estimated labor hours lower bound	Developer salary (per hour)	Projected products
Task 1	160	$100.28	545

Example Calculation:
160 hours × $100.28 × 545 products = $8,744,416.

TABLE 10—TOTAL COST TO DEVELOP AND MAINTAIN THE ELECTRONIC HEALTH INFORMATION EXPORT CRITERION

[2016 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (545 products)	$8,744,416	$87,444,160
Task 2 (545 products)	4,372,208	43,722,080
Task 3 (545 products)	4,372,208	43,722,080
Total (545 products)	17,488,832	174,888,320

Based on the stated assumptions and costs outlined in Table 8, the total estimated cost for health IT developers to develop products to the electronic health information export certification criterion will range from $17.5 million to $174.9 million. Assuming 458 health IT developers, there would be an average cost per health IT developer ranging from $38,185 to $381,852. The midpoint of ranges stated is used as the primary estimate of costs and benefits. We note that the development costs, which equal half of the total, would be a one-time cost and would not be perpetual.

Benefits

There are a number of benefits to the electronic health information export functionality. In our analysis, we have calculated the benefits in terms of the reduced costs of the electronic health information export functionality compared to performing data export without the electronic health information export functionality. The benefit calculations below are based on the following assumptions:

1. *On average, 5% of providers and hospitals switch their health IT annually.* Using CMS Medicare EHR Incentive Program data from years 2013–2016, we estimate the rate of providers (hospitals and eligible professionals) that changed their health IT developer. We believe that the electronic health information export functionality would help alleviate the burden of switching between health IT systems by making data more portable. Thus, the benefit calculations are based on assumptions regarding the number of clinical practices (n = 4,774) and hospitals (n = 226) that are projected to switch products in a year.

2. *Health IT consultants*[164] *will use the same labor costs and data models.* Table 11 shows the estimated labor costs per product for a hospital or health care provider to hire a health IT consultant to perform data export without the electronic health information export functionality. We recognize that these costs will vary based on the size of the hospital or clinical practice.

3. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a ‘‘Software Developer’’ is $50.14.[165]

[164] ‘‘Health IT consultant’’ refers to a technical expert that a hospital or provider will hire to migrate their data from a legacy system to a new EHR.

[165] *https://www.bls.gov/oes/2016/may/oes439061.htm.*

TABLE 11—COST PER PROVIDER TO PERFORM DATA EXPORT WITHOUT ELECTRONIC HEALTH INFORMATION EXPORT FUNCTIONALITY WHEN SWITCHING HEALTH IT PRODUCTS

Activity	Estimated cost per health IT switch (lower bound) (hour)	Estimated cost per health IT switch (upper bound) (hour)	Remarks
Task 1: Understanding and mapping the data in health IT database into standard terms.	320	3,200	The lower bound is an estimate for a small provider practice using the standard instance of a certified health IT product with no customization and use of nationally recognized content standards. The upper bound estimates a medium to large practice with substantial local customization of content.
Task 2: Exporting the data from the health IT into a format that can be subsequently used to import.	160	1,600	The lower bound assumes that the certified health IT product is capable of exporting most of the data into standard output format such as C–CDA. The upper bound estimates the case where a large amount of data is not easily exported by the certified health IT product and therefore substantial one-off software needs to be written to export the data into a custom (de novo) format developed for the transition.
Total Labor Hours	480	4,800	

Table 12 provides an example calculation for how we calculated our total costs presented in table 13.

TABLE 12—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO PROVIDERS TO HIRE A HEALTH IT CONSULTANT TO PERFORM TASK 1 WITHOUT THE ELECTRONIC HEALTH INFORMATION FUNCTIONALITY

[2016 Dollars]

	Estimated labor hours lower bound	Developer salary (per hour)	Estimated annual number of health IT switches
Task 1	320	$100.28	5,000

Example Calculation

320 hours × $100.28 × 5,000 switches = $160,448,000

TABLE 13—TOTAL COST TO PROVIDERS TO PERFORM DATA EXPORT WITHOUT THE ELECTRONIC HEALTH INFORMATION EXPORT FUNCTIONALITY WHEN SWITCHING HEALTH IT PRODUCTS

[2016 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1	$160,448,000	$1,604,480,000
Task 2	80,224,000	802,240,000
Total Cost Savings (5,000 switches)	240,672,000	2,406,720,000

We multiplied the costs to switch health IT by the estimated number of hospitals and clinical practices affected. Thus the estimated annual benefit, in terms of cost savings to hospitals and clinical practices would range from $240.7 million to $2.4 billion. If we assume, based on our upper bound estimates above, that the total cost to health IT developers is $174.9 million and that increased developer costs are passed to customers, then the net benefit to hospitals and clinical practices would range from $65.8 million to $2.2 billion. The midpoint of ranges stated is used as the primary estimate of costs and benefits.

2.3 Application Programming Interfaces

Our proposals regarding APIs in this proposed rule reflect the full depth and scope of what we believe is necessary to implement the API Condition of Certification. We propose to include new standards, new implementation specifications, and a new certification criterion. Our proposal also includes a detailed Condition of Certification and associated Maintenance of Certification requirements, as well as a proposal to modify the Base EHR definition.

Costs

This section describes the potential costs of the API certification criterion. The cost estimates below are based on the following assumptions:

1. *Health IT developers will use the same labor costs and data models.* Table 14 shows the estimated labor costs per

product for a health IT developer to develop and maintain an API. We recognize that health IT developer costs will vary; however, we have assumed in our calculations that all health IT developers will incur the costs noted in Table 14.

2. *A proxy is needed to project number of 2015 Edition certified health IT products containing the API certification criterion.* We estimate that 459 products from 394 developers will contain the API criterion. We used a proxy to determine the number of health IT developers that may develop an API for the certification to the 2015 edition. There were 598 products and 506 developers with at least one 2014 Edition certified health IT product that could perform transitions of care. We then multiplied this number by our certified health IT market consolidation estimates of −22.1% and −23.2% to project the number of 2015 developers and products, respectively. We believe this estimate serves as a reasonable proxy for products capability of sending patient data. The 2015 Edition required API functionality achieves a similar end by allowing providers to retrieve patient data from secure data servers hosted by other developers, as well as providing patients access to their medical records through third-party applications connected to these same secure servers.

3. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $50.14.[166]

TABLE 14—ESTIMATED LABOR HOURS TO DEVELOP AND MAINTAIN API

Tasks	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 1: Develop support for Fast Healthcare Interoperability Resources (FHIR®) API and ARCH 1.0 (per product).	(1) New development to support ''Clinical Notes'', ''Provenance'', ''Address'' and ''Telecon''. (2) Only ''Mandatory'' and ''Must Support'' elements are required for each of the ARCH resources.	1,500	3,500	(1) Lower bound assumes health IT already has developed FHIR DSTU2 and SMART for 2015 and only needs to be updated for additional resources. (2) Upper bound assumes new development for all resources.
Task 2: Development of App registration Server and Portal (per developer).	(1) New registration server development (or updates to existing server) to support registration timeliness and publication of FHIR endpoints. (2) Development of portal and managing the application registration system.	1,000	2,500	(1) Lower bound assumes that the developer already has existing application registration infrastructure in place, and only needs to update it to support the API Maintenance of Certification requirements. (2) Upper bound is new development of an application registration service and portal.
Task 3: Update ARCH and FHIR standards as part of regular API maintenance (per product).	(1) This is an estimate for adding one or two new data elements to USCDI and making it a requirement. (2) Support for API-enabled services for data on a single patient and multiple patients, as well as SMART Backend Services as part of FHIR 4.	1,200	2,000	(1) Lower bound assumes developers are already supporting the elements and also have been testing API-enabled services for data on a single patient and multiple patients. (2) Upper bound assumes new development for USCDI updates and API-enabled services for data on a single patient and multiple patients.
Task 4: Update Application Registration Server and Portal (per developer).	This would be yearly updates and maintenance of the portal to keep it running. We do not anticipate any major changes to the standard and will be primarily driven by usage and developer interest.	400	1,300	(1) Lower bound estimates hours to keep it running with junior staff. (2) Upper bound estimates small updates and adds in developer and quality assurance resources.
Other costs (50% per product, 50% per developer).	(1) Server costs. (2) Software costs (*e.g.,* databases, application servers, portal technology).	$5,000	$25,000	(1) Estimated as monetized costs and not as hours; most of the costs would be one-time procurement costs plus yearly maintenance. *Note: One-time cost.*

Table 15 provides an example calculation for how we calculated our total costs presented in Table 16.

[166] *https://www.bls.gov/oes/2016/may/oes439061.htm.*

TABLE 15—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO DEVELOPERS TO PERFORM TASK 1 TO DEVELOP API

[2016 Dollars]

	Estimated labor hours lower bound	Developer salary (per hour)	Projected products
Task 1	1,500	$100.28	459

Example Calculation:
1,500 hours × $100.28 × 459 products = $69,042,780

TABLE 16—TOTAL COST TO DEVELOP AND MAINTAIN API

[2016 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (459 products)	$69,042,780	$161,099,820
Task 2 (394 developers)	39,510,320	98,775,800
Task 3 (459 products)	55,234,224	92,057,040
Task 4 (394 developers)	15,804,128	51,363,416
Other Costs (394 developers)	985,000	4,925,000
Other Costs (459 products)	1,147,500	5,737,500
Total (459 products and 394 developers)	181,723,952	413,958,576

We note that we have proposed to adopt in § 170.404(b)(3) a specific requirement that an API Technology Supplier must support the publication of Service Base URLs for all of its customers regardless of whether they are centrally managed by the API Technology Supplier or locally deployed. The API Technology Supplier must make such information publicly available at no charge. Thus, we are placing the responsibility of publishing the URLs on health IT developers and those costs are captured in the registration portal cost estimation in this RIA.

Based on the stated assumptions and costs outlined in Table 16, the total estimated costs for health IT developers to develop and maintain a product to the API criterion would range from $181.7 million to $414.0 million with an average cost per developer ranging from $461,228 to $1,050,656. We note that the ''other costs,'' which account for $2.1 million to $10.7 million of this total are one-time costs and are not perpetual. The midpoint of ranges stated is used as the primary estimate of costs and benefits.

Benefits

The Medicare Access and CHIP Reauthorization Act (MACRA) tasks ONC with measuring interoperability in the health IT industry.[167] The measurement concepts developed include a multi-part approach analyzing not only adoption of health IT functionalities supporting information exchange but the downstream impact of these technologies on data completeness, data integration, and supports for core functions of patient care. The benefits of our API proposal are similarly multifaceted. In the analysis below, we quantify benefits in the following three areas:

- Reduction in provider burden associated with locating patient data;
- Reduced costs related to reductions in duplicate lab tests, readmissions, emergency room (ER) visits, and adverse drug events due to increased interoperability. We focused on these outcomes for two reasons: (i) Evidence in literature indicates that health information exchange impacts the chosen measures; and (ii) cost of care associated with these measures is high and the impact of health information exchange is likely to result in significant benefits in the form of cost reduction.
- Increase in the number of individuals with access to their health information.

The benefit calculations are based on the following assumptions:

1. *Benefits noted in academic literature are assumed accurate.* Estimates of the benefits are based on estimates obtained from peer reviewed academic literature. ONC reviewed academic articles for validity; however, models were not replicated.

2. *Hospitals and eligible professionals that have participated in the CMS EHR Incentive Programs will be impacted:* Estimates are based on the assumption that 439,187 health care providers and/or 4,519 hospitals would be affected by this regulatory action.

3. *Estimates on the impact of APIs on rates of interoperability (1% to 4%) are based on ONC analysis.* To identify the impact of the API proposal on interoperability, we used regression analysis. Specifically, we estimated linear probability models that identified the impact of 2014 Edition certified EHR on hospitals' interoperability (whether a hospital sends, receives, finds, and integrates summary of care records). Using data from the American Hospital Association (AHA) from years 2014 to 2015 in the model, we controlled for hospital size, profit status, participation in a health information organization, and state and year fixed effects. The marginal effect of using a 2014 Edition certified health IT equated to a 5% increase in interoperability. This is an upper bound estimate. For the purpose

[167] Health IT Buzz Blog, *Measuring Interoperability: Listening and Learning, https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/interoperability-electronic-health-and-medical-records/measuring-interoperability-listening-learning/.*

of this analysis, we assume that one to four percentage points would be a reasonable range for API's marginal impact on interoperability.

As noted previously, there might be shared benefits across certain proposals and we have taken steps to ensure that the benefits attributed to each proposal are unique to the proposal referenced. Specifically, we used regression analysis to calculate the impact of our real world testing and API proposals on interoperability. We assumed that the collective impact of real world testing and API proposals on interoperability would not exceed the impact of 2014 Edition certified health IT. Therefore, we estimated linear probability models that identified the impact of 2014 Edition certified health IT on hospitals' interoperability.[168] We controlled for additional factors such as participation in a health information exchange organization, hospital characteristics, and urban/rural status. We found the marginal effect of using 2014 Edition certified health IT was a five percentage point increase in interoperability.

While we acknowledge that there might be shared benefits across proposals, we have taken steps to ensure that the benefits attributed to each proposal is unique to the proposal referenced. We assumed that this marginal effect is true for our proposals and distributed the 5% benefit across our real world testing and API proposals at (.1–1%) to (1–4%) respectively. Moreover, the number of providers impacted is proposal specific. Given data limitations, we believe this approach allows us to estimate the benefits of our proposals without double counting the impact each proposal might have on interoperability.

The first table below shows benefits of APIs for providers where we monetize the impact of APIs as total amount saved by reducing provider time spent with the health IT. Sinsky et al found physicians spend 27% of their total time on direct clinical face time with patients, and 49.2% of their time on EHR and desk work.[169] Outside office hours, physicians spend another 1 to 2 hours of personal time each night doing additional computer and other clerical work. Based on this study, we assume that providers spend, on average, 6 hours per day with their EHR (4 hours of an 8 hour work day and 2 hours outside of office hours). Despite the number of hours providers spend in their EHR, there is evidence that the introduction of EHRs is associated with time saved. Amusan et al found that EHR and computerized provider order entry (CPOE) implementation was associated with 3.69 minutes of time saved five months post implementation.[170] Additionally, Adler-Milstein et al found that an increase in EHR use resulted in a 5.3% increase in work relative value units per clinician work day.[171] Using this evidence, we estimate the potential impact of APIs on providers' time ranges from 1%–5%.[172] Because the benefit of time saved is not limited to interoperable exchange of health information among providers but includes additional benefits such as increased patient knowledge, we used evidence from the literature to calculate the time saved benefit. Thus, the impact of APIs on provider time is expected to represent a larger impact (5%) than the impact of APIs on health outcomes (1%–4%) and cost. This is primarily because provider behavior is more directly affected by this improvement.

Benefits of APIs

TABLE 17—BENEFIT OF API PROVIDERS

[2016 Dollars]

Benefit type	Number affected	Hourly wage	Hours saved (percent) [a] [b]		Hours per day with EHR	Number of working days in a year	Total benefit [c] (per year)	
			Min	Max			Min	Max
Reduction in provider time spent in health IT by improving usability and interoperability.	439,187 providers	95	1	5	[d] 6	260	$651M	$3.3B

[a] Julia Adler-Milstein and Robert S. Huckman, The Impact of Electronic Health Record Use on Physician Productivity, Am J Manag Care (Nov. 19, 2013).

[b] Amusan, Tongen, Speedie, and Mellin, A time-motion study to evaluate the impact of EMR and CPOE implementation on physician efficiency, J. Healthcare Inf. Manag. (Fall 2008), at 31–7.

[c] Total benefit is a product of *number affected physicians, hourly wage, hours saved from EHR improvements, hours worked with EHR,* and *number of working days in a year.*

[d] Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties,* Ann Intern Med. (Dec. 6, 2016), at 753–60.

TABLE 18—BENEFIT OF API FOR PATIENTS AND PAYERS

[2016 Dollars]

Benefit type	Number affected	Overall interop impact (marginal effect)	Impact of API		Total cost	% of total cost impacted	Total benefit [a] (per year)	
			Min	Max			Min	Max
Duplicate testing	439,187 providers	[b] 0.09	0.01	0.04	[c] 200 Billion.	100	$180M	$720M
Avoidable hospitalizations and readmissions.	4,519 hospitals	[b] 0.09	0.01	0.04	[d] $41B	100	37M	148M

[168] American Hospital Association Health IT Supplement Survey, *http://www.ahadata.com/aha-healthcare-database/.*

[169] Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties,* Ann Intern Med. (Dec. 6, 2016), at 753–60.

[170] Amusan, Tongen, Speedie, and Mellin, A time-motion study to evaluate the impact of EMR and CPOE implementation on physician efficiency, J. Healthcare Inf. Manag. (Fall 2008), at 31–7.

[171] Julia Adler-Milstein and Robert S. Huckman, The Impact of Electronic Health Record Use on Physician Productivity, Am J Manag Care (Nov. 19, 2013).

[172] The calculation for these estimates are as follows: 1% leverages Amusan et al.'s lower bound estimate of 3.69 minutes. Assuming 6 hours (or 360 minutes) per day, this amounts to approximately 1% of time saved. The upper bound estimate of 5% leverages Adler-Milstein's estimate of a 5.3% estimate (rounded to 5%).

TABLE 18—BENEFIT OF API FOR PATIENTS AND PAYERS—Continued

[2016 Dollars]

Benefit type	Number affected	Overall interop impact (marginal effect)	Impact of API		Total cost	% of total cost impacted	Total benefit[a] (per year)	
			Min	Max			Min	Max
E visits	100% of visits affected	[b] 0.09	0.01	0.04	[e] Cost per ER visit $1,233, 131M visits.	100	48M	194M
Adverse drug events	20% of events affected	[f] 22%	0.01	0.04	[g] $30 billion.	20	13M	53M

[a] Total benefit is a product of *total cost, % of total cost impacted, overall impact of interoperability, and impact of API.*

[b] Stephen E. Ross, Tiffany A. Radcliff, William G. Leblanc, L. Miriam Dickinson, Anne M. Libby, and Donald E. Nease Jr., Effects of health information exchange adoption on ambulatory testing rates, J. Am. Med. Inform. Assoc. (2013), at 1137–1142; Bridget A. Stewart, Susan Fernandes, Elizabeth Rodriguez-Huertas, and Michael Landzberg, A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients, J. of the Am. Med. Informatics Assoc. (2010), at 341–344; Sezgin Ayabakan, Indranil R. Bardhan, Zhiqiang (Eric) Zheng, and Kirk Kirksey Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals, MIS Quarterly (Jan. 1, 2017); Eric J. Lammers, Julia Adler-Milstein, and Keith E. Kocher, Does health information exchange reduce redundant imaging? Evidence from emergency departments, Med Care (Mar. 2014), at 227–34.

[c] National Academy of Medicine. (2016), *http://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html.*

[d] Agency for Healthcare Research and Quality (AHRQ) Statistical Brief #199 (Dec. 2015), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb199-Readmissions-Payer-Age.pdf;* AHRQ Statistical Brief #72, Nationwide Frequency and Costs of Potentially Preventable Hospitalizations (Apr. 2009), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb72.pdf.*

[e] National Center for Health Statistics (NCHS) Data Brief No. 252 (June 2016), *https://www.cdc.gov/nchs/data/databriefs/db252.pdf;* Nolan Caldwell, Tanja Srebotnjak, Tiffany Wang, and Renee Hsia, "How Much Will I Get Charged for This?" Patient Charges for Top Ten Diagnoses in the Emergency Department (2013), *https://doi.org/10.1371/journal.pone.0055491.*

[f] M.F. Furukawa, W.D. Spector, M.R. Limcangco, and W.E. Encinosa, Meaningful use of health information technology and declines in in-hospital adverse drug events, J. of the Am. Med. Informatics Assoc. (2017).

[g] Janet Sultana, Paola Cutroneo, and Gianluca Trifirò, *Clinical and economic burden of adverse drug reactions.*

Based on the above calculations, we estimate the annual benefit to health care providers for the use of the proposed API capabilities would, on average, range from $651 million to $3.3 billion. We estimate the annual benefit for patients and payers would, on average, range from $278 million to million to $1.1 billion. Therefore, we estimate the total annual benefit of APIs to, on average, range from $929 million to $4.4 billion. If we assume, based on our cost estimates, an annual cost to health IT developers of $414 million and that increased developer costs are passed to customers, then the net benefit to hospitals/providers would range from $515 million to $3.3 billion. The midpoint of ranges stated is used as the primary estimate of benefits.

As we stated above, for Table 17, we assume APIs provide both patients and clinicians with increased access to EHI, which will have a direct impact on physicians by making their work more efficient. Extrapolating the numbers from literature, we assume this technology will improve physicians' time by 1%–5%. Also as stated above, for Table 18, we assume APIs affect utilization through marginal improvements in interoperability. For this reason, in addition to APIs, we needed to incorporate the impact of interoperability on each of the outcomes. We request comment on these assumptions. Specifically, whether they are appropriate and whether there are alternative assumptions or bases upon which we should make our assumptions.

We expect additional benefits from the use of APIs could be derived from increased patient, and eventually payer, access to EHI. APIs make it easier for patients to transmit data to and from different sources. According to the Health Information National Trends Survey,[173] half of Americans were offered access to an online medical record by a provider or insurer in 2017. However, among those who were offered access, only 53% accessed their record at least once within the last year, and only 3.6% of individuals who accessed their record reported transmitting their data to a service or application. The proportion of individuals accessing their online health information and transmitting their information to third parties is expected to grow as APIs become more widespread and make more data available in a computable format. Growing evidence suggests that patients who have access to their EHI are more likely to adhere to medical orders including screening recommendations.[174] Thus, we expect such patients would ultimately realize improved health outcomes.

In addition, the use of APIs to support the exchange and analysis of payment related data (including price information) would improve cost transparency in the market, increase the availability of valuable information for payers and patients, and likely drive down health care prices. For instance, a recent study by the Minnesota Department of Health showed that the pricing for knee replacement surgery, which is a standard procedure in many hospitals, can vary significantly across practices in the same locality. The Minnesota study showed that Minnesota insurers paid as much as $47,000 for a patient's total knee replacement and as little as $6,200—a nearly eight-fold price difference. In addition to total knee replacements, the study found that total hip replacement costs ranged from $6,700 to $44,000, a 6½-fold difference. Typical vaginal baby delivery ranged from $2,900 to $12,300, while C-section deliveries ranged from $4,700 to $22,800. Another study by Premier in conjunction with Wake Forest University Medical Center found similar results. Among 350 hospitals, the average cost of primary knee implants was $4,464. Yet, 50% of the hospitals paid between $4,066 and $5,609 on the devices. Further, the same group of hospitals paid an average of $5,252 for primary hip implants, but 50% of the hospitals paid between $4,759 and $6,463. The studies illustrated the secretive nature of pricing in the health care market, as well as the extreme variations in price that can exist for the same procedure within the same locality.[175] [176] While this study was the

[173] These estimates were derived from Health Information National Trends Survey 5, Cycle 1 (2017).

[174] *See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5391175/.*

[175] Glenn Howatt, *That surgery will cost you $6,200. Or maybe $47,000,* Star Tribune (Jan. 3, 2018), *available at http://www.startribune.com/that-surgery-will-cost-you-6-200-or-maybe-47-000/467894173/.*

[176] Bakalar, Catherine and Czajka, Robin (2018) Margin of Excellence: Total Joint Replacements

first-ever local study of insurance company payments to hospitals for those four common procedures, similar pricing variations have been well documented in other, broader studies in recent years.[177] We expect that making such price information available to insurers through APIs would drive health care prices down, which could lead to significant benefits across the health care continuum.

While the examples above emphasize procedures that tend to have defined end points, the eventual population health queries would more broadly allow payers and analytics firms working for employers to computationally examine the care providers render. Not only is price transparency currently missing from the marketplace, but for most inpatient care, the actual details of care are largely unobtainable through any APIs. However, we are not aware of an approach for quantifying these types of benefits and welcome comments on potential approaches to quantifying these benefits.

2.4 New Privacy and Security Certification Criteria

To be certified to the new privacy and security certification criteria, encrypt authentication credentials (§ 170.315(d)(12)) and multi-factor authentication (MFA) (§ 170.315(d)(13)), we are proposing to require health IT developers to assess their Health IT Modules' capabilities and attest ''yes'' or ''no'' to the certification criteria. As specified in section IV.C.3 of this proposed rule, we are proposing to make these certification criteria applicable to all Health IT Modules under the Program. For encrypt authentication credentials and multi-factor authentication, we are proposing to require a simple attestation. For MFA, we are also proposing to require that if the health IT developer attests to supporting MFA, the health IT developer would need to explain how it supports MFA. We also request public comment on whether there is value in adopting an MFA criterion and whether the health IT developer should explain how it supports MFA.

Costs

These criteria are not intended to place additional burden on health IT developers as they do not require new development or implementation. Rather, a health IT developer is only required to attest to whether they encrypt authentication credentials or support MFA. We expect the costs associated with attesting to these criteria to be de minimis because we do not expect additional forms to be required and expect minimal effort would be required to complete the attestation. We welcome comments on these expectations. The midpoint of ranges stated is used as the primary estimate of costs and benefits.

Benefits

As stated previously, we are not requiring health IT developers to encrypt authentication credentials or support MFA. Instead, we are requiring they attest to whether they support the certification criteria or not. By requiring an attestation, we are promoting transparency, which might motivate some health IT developers that do not currently encrypt authentication credentials or support MFA to do so. If health IT developers are motivated by this criteria and ultimately do encrypt authentication credentials and/or support MFA, we acknowledge that there would be costs to do so; however, we assume that the benefits would substantially exceed the costs. Encrypting authentication credentials and adopting MFA would reduce the likelihood that authentication credentials would be compromised and would eliminate an unnecessary use of IT resources. Encrypting authentication credentials and adopting MFA could directly reduce providers' operating/support costs, which would reduce their administrative and financial burden. Encrypting authentication credentials would also help decrease costs and burden by reducing the number of password resets due to possible phishing or other vulnerabilities.

According to Verizon's 2017 Data Breach Investigations Report, 81% of hacking-related breaches leveraged either stolen and/or weak passwords.[178] The Verizon report encourages customers to vary their passwords and use two-factor authentication. Also, NIST Special Publication 800–63B: Digital Identity Guidelines, *Authentication and Lifecycle Management,*[179] recommends the use of and provides the requirements for using multi-factor authenticators. Based on these reports and other anecdotal evidence, we believe encrypting authentication credentials and supporting MFA are established best practices among industry developers, including health IT developers. As described above, we propose to require health IT developers to attest to whether they encrypt authentication credentials. We do not have access to published literature that details how health IT developers are already encrypting authentication credentials and supporting MFA industry-wide, but we believe the majority of health IT developers, or around 80%, are taking such actions. We assume that building this functionality is in the future project plans for the remaining 20% because, as noted previously, adopting these capabilities is an industry best practice. Health IT developers that have not yet adopted these capabilities are likely already making financial investments to get up to speed with industry standards. We believe our proposal may motivate these health IT developers to speed their implementation process, but we have not attributed a monetary estimate to this potential benefit because our rule is not a direct cause of health IT developers adopting these capabilities. By the time we release the final rule, many more, or perhaps all, health IT developers will likely already be encrypting authentication credentials and supporting MFA. We welcome comments on this expectation and any means or methods we could use to quantify these benefits.

2.5 Data Segmentation for Privacy-Send and Data Segmentation for Privacy-Receive; and Consent Management for APIs

We propose to remove the current 2015 Edition Data Segmentation for Privacy (DS4P)-send (§ 170.315(b)(7)) and DS4P-receive (§ 170.315(b)(8)) certification criteria which apply the DS4P standard at the document level. We propose to replace these two criteria with three new 2015 Edition DS4P certification criteria (two for C–CDA and one for FHIR) that would support a more granular approach to privacy tagging data for health information exchange supported by either the C–CDA- or FHIR-based exchange standards. In place of the removed 2015 Edition DS4P criteria, we propose to adopt new DS4P-send (§ 170.315(b)(12)) and DS4P-receive (§ 170.315(b)(13))

[White Paper] May 24, 2018, *http://offers.premierinc.com/rs/381-NBB-525/images/WC_CM_TotalJoint_2018_05_04.pdf.*

[177] *See e.g.,* Elisabeth Rosenthal, *The $2.7 Trillion Medical Bill; Colonoscopies Explains Why U.S. Leads the World in Health Expenditures,* The New York Times (June 1, 2013), *available at http://www.nytimes.com/2013/06/02/health/colonoscopies-explain-why-us-leads-the-world-in-health-expenditures.html?pagewanted=all*; Steve Twedt, *Hospitals' charges can vary greatly for similar services,* Pittsburgh Post-Gazette (May 9, 2013), *available at http://www.post-gazette.com/business/businessnews/2013/05/09/Hospitals-charges-can-vary-greatly-for-similar-services/stories/201305090300.*

[178] *http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.*

[179] *https://pages.nist.gov/800-63-3/sp800-63b.html.*

criteria that would remain based on the C–CDA and the HL7 DS4P standard. These criteria would include capabilities for applying the DS4P standard at the document, section, and entry level. We also propose to adopt a third 2015 Edition DS4P certification criterion ''consent management for APIs'' (§ 170.315(g)(11)) that requires health IT to be capable of responding to requests for data through an API in accordance with the Consent Implementation Guide. Our primary purpose for proposing to remove and replace them, in lieu of proposing to revise them, is to provide clarity to stakeholders as to the additional functionality enabled by health IT certified to the new criteria.

Costs

We anticipate this proposal could result in up-front costs to health IT developers as this new criteria would require the health IT to support all three levels—document, section, and entry—as specified in the current DS4P standard. However, we note that these criteria are not being required in any program at this time. As of the beginning of the third quarter of the 2018 CY, only about 20 products (products with multiple certified versions were counted once) were certified to the current 2015 Edition DS4P certification criteria. We estimate that 10–15 products will implement the new DS4P criteria. Developers may need to perform fairly extensive health IT upgrades to support the more complex and granular data tagging requirements under these criteria. We anticipate developers will need approximately 1,500–2,500 hours to upgrade databases and/or other backend infrastructure to appropriately apply security labels to data and/or develop access control capabilities. Moreover, developers will likely incur costs to upgrade health IT to generate a security-labeled C–CDA conforming to the DS4P standard. We estimate developers will need 400–600 hours per criterion to make these upgrades on systems that had previously certified to the document-level DS4P criteria, or 720–1,220 hours per criterion for systems that are implementing these criteria for the first time. We believe this work would be performed by a ''Software Developer.'' According to the May 2016 BLS occupational employment statistics, the mean hourly wage for software developer is $50.14. As noted previously, we have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages, so the hourly wage including overhead costs is $100.28. Therefore, we estimate the total cost to developers could range from $2,306,440 to $7,430,748. We note that this would be a one-time cost. The midpoint of ranges stated is used as the primary estimate of costs and benefits.

Additionally, our proposal supports the capability to respond to requests for patient consent information through an API compatible with FHIR Release 3. In order to meet the ''consent management for APIs'' criteria, developers would demonstrate compatibility with the standards framework used for the Consent Implementation Guide. We have estimated costs associated with this aspect of our proposal using the following assumptions:

1. We estimate developers will require 1,500–3,500 hours to upgrade health IT to align with the FHIR STU3 data model and develop a STU3 compatible FHIR server.

2. As with the two DS4P criteria, we anticipate developers will need approximately 1,500–2,500 hours to upgrade databases and/or other backend infrastructure to appropriately apply security labels to data and/or develop access control capabilities. We expect that this would be a one-time cost.

3. Because certification to this criterion is voluntary and because supporting this criterion requires implementation of a version of FHIR (STU3) that does not align with the other API criterion in this rule (based on DSTU2), we estimate the number of products that will support this criterion is approximately 5% of the total number of 2015 certified products. We used a proxy to determine the number of health IT developers that may develop an API for the 2015 Edition. There were 598 products and 506 developers with at least one 2014 Edition certified product that could perform transitions of care. We then multiplied this number by our certified health IT market consolidation estimates of −22.1% and −23.2% to project the number of 2015 developers and products, respectively; we estimate that 459 products from 394 developers will contain the API criterion. Therefore, we anticipate 23 products from 20 developers will certify to the ''consent management for APIs'' criterion. We believe this work would be performed by a ''Software Developer.''

4. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $50.14.

Our cost estimates are explained in the table below.

TABLE 19—COSTS RELATED TO DATA SEGMENTATION FOR PRIVACY USING API

[2016 Dollars]

Tasks	Details	Lower bound hours	Upper bound hours	Assumptions	Remarks
Task 1: Enhance health IT to align with the FHIR STU3 data model and develop a STU3 compatible FHIR server.	Enhance health IT to align with the FHIR STU3 data model and develop a STU3 compatible FHIR server.	1,500	3,500	....	This is a one-time cost for health IT systems to align with the FHIR STU3 data model and develop a STU3 compatible FHIR server.
Task 2: Enhancements to health IT to upgrade databases and/or other backend infrastructure to appropriately apply security labels to data and/or develop access control capabilities.	Enhancements to health IT to upgrade databases and/or other backend infrastructure to appropriately apply security labels to data and/or develop access control capabilities.	1,500	2,500	....	This is a *one-time cost* for health IT systems to support data segmentation for discrete data.
Total Labor Hours	....	3,000	6,000		
Hourly Rate	....	$100.28			

TABLE 19—COSTS RELATED TO DATA SEGMENTATION FOR PRIVACY USING API—Continued

[2016 Dollars]

Tasks	Details	Lower bound hours	Upper bound hours	Assumptions	Remarks
Cost per Product		$300,840	$601,680		
Total Cost (23 products)		$6,919,320	$13,838,640		

We believe this proposal involving standardized APIs, as well as the voluntary nature of the proposal, would significantly mitigate health IT developer costs. We also expect developers to see a return on their investment in developing and preparing their health IT for these certification criteria given the benefits to interoperable exchange. We welcome comments on this analysis.

We anticipate potential costs for ONC related to this proposal associated with: (1) Developing and maintaining information regarding these new criteria on the ONC website; (2) creating documents related to these new criteria and making those documents 508 compliant; (3) updating, revising, and supporting Certification Companion Guides, test procedures, and test tools; and (4) responding to inquiries concerning these criteria. We estimate an ONC analyst at the GS–13, Step 1 level staff would devote, on average, 200 hours to the above tasks annually. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate the annual costs to be $17,660.

Benefits

We believe leveraging the DS4P standard's ability to allow for both document level and more granular tagging would offer functionality that is more valuable to providers and patients, especially given the complexities of the privacy landscape for multiple care and specialty settings. We also believe this proposal would benefit providers, patients, and ONC because it would support more complete records, contribute to patient safety, and enhance care coordination. We believe this proposal could also reduce burden for providers by enabling an automated option, rather relying on case-by-case manual redaction and subsequent workarounds to transmit redacted documents. We emphasize that health care providers already have processes and workflows to address their existing compliance obligations, which could be made more efficient and cost effective through the use of health IT. We expect these benefits for providers, patients, and ONC to be significant; however, we are unable to quantify these benefits at this time because we do not have adequate information to support quantitative estimates. We welcome comments regarding potential approaches for quantifying these benefits.

(3) Conditions and Maintenance of Certification

3.1 Information Blocking

For a discussion of the costs and benefits of the exceptions to information blocking proposed in this rule, please see section (5) of this RIA.

3.2 Assurances

We are proposing that health IT developers must make certain assurances as Conditions and Maintenance of Certification: (1) Assurances regarding the electronic health information export certification criterion in § 170.315(b)(10) and (2) assurances regarding retaining records and information.

3.2.1 Electronic Health Information Export

We propose, as a Condition of Certification requirement, that a health IT system that produces and electronically manages electronic health information must be certified to the 2015 Edition ''electronic health information export'' certification criterion in § 170.315(b)(10). Further, as a Maintenance of Certification requirement, health IT developers must comply with this proposed Condition of Certification requirement within 24 months of a subsequent final rule's effective date or at the time of certification if the health IT developer never previously certified health IT to the 2015 Edition. As another Maintenance of Certification requirement, we propose that health IT developers must provide all of their customers with the functionality included in § 170.315(b)(10).

For a detailed discussion of the costs and benefits of the assurances regarding the electronic health information export certification criterion in § 170.315(b)(10), please see section 2.2 of this RIA above.

3.2.2 Records and Information Retention

We propose that, as a Maintenance of Certification requirement, a health IT developer must, for a period of 10 years beginning from the date of certification, retain all records and information necessary that demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program. In an effort to reduce administrative burden, we also propose, that in situations where applicable certification criteria are removed from the Code of Federal Regulations before the 10 years have expired, records must only be kept for 3 years from the date of removal for those certification criteria and related Program provisions unless that timeframe would exceed the overall 10-year retention period. This ''3-year from the date of removal'' records retention period also aligns with the records retention requirements for ONC–ACBs and ONC–ATLs under the Program.

Currently, there are no existing regulatory requirements regarding record and information retention by health IT developers. We expect the costs to developers to retain the records and information described above to be mitigated due to the following factors. First, we expect that health IT developers are already keeping the majority of their records and information in an electronic format. Second, we expect that health IT developers already have systems in place for retaining records and information. Last, we expect that some developers may already be retaining records and information for extended periods of time due to existing requirements of other programs, including for those programs their customers participate in. For instance, Medicaid managed care companies are required to keep records for ten years from the effective date of a contract.

We estimate that each health IT developer will, on average, spend two hours each week to comply with our proposed record retention requirement. We expect that a health IT developer's office clerk could complete the record retention responsibilities. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for an office clerk is $15.87.[180] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages, so the hourly wage including overhead costs is $31.74. Therefore, we estimate the annual cost per developer would, on average, be $3,301 and the total annual cost for all health IT developers (458 health IT developers have products certified to the 2015 Edition that are capable of recording patient health data) would, on average, be $1.5 million. We note that this is a perpetual cost. We welcome comments on these cost estimates.

3.3 Prohibition or Restriction of Communications Costs

Health IT developers would need to notify their customers about the unenforceability of communications and contract provisions that violate this Condition of Certification. Generally, health IT developers should already have mechanisms in place, whether via online postings, email, mail, or phone, for alerting customers to changes in their policies and procedures. Such alerts should be standard practice. However, we have estimated the potential costs for health IT developers to draft the notice and mail the notice as appropriate. We estimate that a health IT developer's office clerk will commit (overall) approximately 40 hours to drafting and mailing notices when necessary. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for an office clerk is $15.87.[181] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages, so the hourly wage including overhead costs is $31.74. Therefore, we estimate the annual cost per developer to be $1,270 and the total cost for all health IT developers (792 health IT developers certified to the 2014 Edition) to be $1 million. We note that this is a one-time cost and would not be perpetual.

We also note that mailing is one option for delivery, along with other means such as email. We do not have information concerning how health IT developers will deliver their notices. We have estimated a total cost for all developers to mail the notices (including postage) to be $80,000. Again, we note that this is a one-time cost. We welcome comments on these cost estimates.

In order to meet the Cures Act requirement that health IT developers do not prohibit or restrict communication regarding health IT, some health IT developers would eventually need to amend their contracts to reflect such a change. Many standard form health IT contracts limit the ability of users to voluntarily discuss problems or report usability and safety concerns that they experience when using their health IT. This type of discussion or reporting is typically prohibited through broad confidentiality, nondisclosure, and intellectual property provisions in the vendor's standard form health IT contract. Some standard form health IT contracts may also include non-disparagement clauses that prohibit customers from making statements that could reflect negatively on the health IT developer. These practices are often referred to colloquially in the industry as ''gag clauses.'' We expect amendments to these clauses to be accomplished in the normal course of business, such as when renegotiating contracts or updating them for HIPAA or other compliance requirements. As such, we do not estimate any direct or indirect costs for health IT developers to amend their contracts to comply with this condition of certification.

Benefits

We expect health care providers to benefit from this proposal. There is growing recognition that these practices of prohibiting or restricting communication do not promote health IT safety or good security hygiene and that health IT contracts should support and facilitate the transparent exchange of information relating to patient care. We are unable to estimate these benefits because we do not have adequate information to determine the prevalence of gag clauses and other such restrictive practices, nor do we have a means to quantify the value to providers of being able to freely communicate and share information. We welcome comments on approaches to quantify these benefits.

3.4 Application Programming Interfaces

For a discussion of the costs and benefits of the new API criterion, please see section 2.3 of this RIA.

3.5 Transparency Requirements for Application Programming Interfaces

We propose as part of the Conditions and Maintenance of Certification that API Technology Suppliers be required to make specific business and technical documentation necessary to interact with the APIs in production freely and publicly accessible. We expect that the API Technology Suppliers would perform the following tasks related to transparency of business and technical documentation and would devote the following number of hours annually to such task: (1) Health Level 7's (HL7®) Fast Healthcare Interoperability Resources (FHIR®) API documentation (the vendor would most likely point to the HL7 FHIR standard for API documentation) (estimated eight hours); (2) patient application registration documentation, which would include a development effort to create a website that manages the application registration activity (estimated 40 hours); (3) publication of the FHIR Endpoint—Base URLs for all centrally managed providers (estimated 40 hours); (4) publication of FHIR Endpoints for provider-managed APIs (estimated 160 hours); and (5) API cost information documentation, which would typically be documented as a tiered rate based on usage or some form of monthly rate (estimated 40 hours).

We believe each of the above tasks would be performed by a ''Software Developer.'' According to the May 2016 BLS occupational employment statistics, the mean hourly wage for software developer is $50.14[182] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages, so the hourly wage including overhead costs is $100.28. Therefore, we estimate the cost per developer to be $28,881. As noted in section 2.3 of this RIA, we estimate that 459 products from 394 developers will contain the API criterion. Therefore, we estimate the total developer total would be $11.4 million. We note that this is a one-time cost and would not be perpetual.

3.6 Real World Testing

The objective of real world testing is to verify the extent to which deployed health IT products in operational production settings are demonstrating compliance to certification criteria and functioning with the intended use cases for continued maintenance of certification. Real world testing should ensure certified health IT products have the ability to share electronic health information between other systems. Real world testing should assess that the certified health IT is meeting the intended use case(s) of the certification criteria to which it is certified within the workflow, health IT architecture,

[180] *See https://www.bls.gov/oes/2016/may/oes439061.htm.*

[181] *See https://www.bls.gov/oes/2016/may/oes439061.htm.*

[182] *See https://www.bls.gov/oes/2016/may/oes439061.htm.*

and care/practice setting in which the health IT is implemented. We note that we expect real world testing would take about three months of the year to perform.

Costs

This section describes the potential costs of the real world testing requirements in this proposed rule. The costs estimates are based on the following assumptions:

1. *Health IT developers will use the same labor costs.* Table 20 shows the estimated labor costs for a health IT developer to perform real world testing. We recognize that health IT developer costs will vary; however, our estimates in this section assume all developers will incur the costs noted in Table 20.

2. *Proxy needed to project the number of 2015 Edition products impacted by real world testing.* We estimate that 523 products from 429 developers will be impacted by real world testing. We used a proxy to determine developers that would be subject to real world testing There were 681 products and 551 developers with at least one of its 2014 Edition certified products that could perform either (or both) transitions of care and/or send any type of public health data. We then multiplied these numbers by our estimates for certified health IT market consolidation by −22.1% and −23.2% to project number of 2015 developers and products, respectively. We believe this estimate serves as a reasonable proxy for products impacted by real world testing, as these products primarily focus on interoperability.

The tables below describe the various costs to health IT developers to perform real world testing by task.

TABLE 20—ESTIMATED COST TO HEALTH IT DEVELOPERS TO PERFORM REAL WORLD TESTING[a]

[2016 Dollars]

Tasks and labor category	Hours	Rate	Total
Task 1: Design Real World Testing Approach and Submit Plan (per developer)			$33,817
15–1133 Software Developers, Systems Software	80	106.34	8,507.20
15–1143 Computer Network Architects	120	100.24	12,028.80
15–1121 Computer Systems Analysts	80	88.10	7,048.00
15–1199 Computer Occupations, All Other	40	85.46	3,418.40
27–3042 Technical Writers	40	70.36	2,814.40
Task 2: Prepare Staff and Environments (per developer)			14,646
15–1121 Computer Systems Analysts	40	88.10	3,524.00
15–1142 Network and Computer Systems Administrators	40	81.26	3,250.40
15–1152 Computer Network Support Specialists	40	65.16	2,606.40
15–1199 Computer Occupations, All Other	40	85.46	3,418.40
15–1122 Information Security Analysts	20	92.34	1,846.80
Task 3: Perform Testing (per product)			31,577
15–1121 Computer Systems Analysts	80	88.10	7,048.00
15–1133 Software Developers, Systems Software	40	106.34	4,253.60
15–1199 Computer Occupations, All Other	160	85.46	13,673.60
15–1142 Network and Computer Systems Administrators	40	81.26	3,250.40
15–1141 Database Administrators	40	83.78	3,351.20
Task 4: Collect Results and Prepare-Submit Report (per developer)			20,118
15–1199 Computer Occupations, All Other	120	85.46	10,255.20
15–1121 Computer Systems Analysts	80	88.10	7,048.00
27–3042 Technical Writers	40	70.36	2,814.40
Total Labor Hours	1,140		
Other Direct Costs—printing, publishing (per product)			150.00
Total Cost			100,307

[a] Labor rates in this chart are from the BLS. *See https://www.bls.gov/oes/2016/may/oes439061.htm.*

TABLE 21—REAL WORLD TESTING TOTAL ANNUAL COST

[2016 Dollars]

Task	Calculation	Total cost
Task 1	$33,817 × 429 developers	$14,507,407
Task 2	$14,646 × 429 developers	6,283,134
Task 3	$31,577 × 523 products	16,514,666
Task 4	$20,118 × 429 developers	8,630,450
Other Direct Costs	$150 × 429 developers	78,450
Total Cost		46,014,108

Based on the stated assumptions and costs outlined in the above tables, we estimate the total annual cost for real world testing would, on average, be $46 million with an average cost per developer of $107,259.

Benefits

There are a number of benefits that can be attributed to real world testing. Real world testing may impact the effective integration of varied health IT systems, including integration of certified health IT with non-certified and ancillary technologies such as picture archiving and communications systems (PACS) or specialty specific interfaces. Real world testing might also have an effect on the effective implementation of workflows in a clinical setting. In this analysis, we have calculated the benefits in the following categories:

1. Provider time saved documenting in their EHR due to improved usability.

2. Increased provider satisfaction with their EHR resulting in fewer providers incurring the costs of switching products.

3. Benefits related to reductions in duplicate lab tests, readmissions, ER visits, and adverse drug events due to increased interoperability. We focused on these outcomes for two reasons: (i) Evidence in literature indicate that health information exchange impacts the chosen measures; and (ii) cost of care associated with these measures is high and the impact of health information exchange is likely to result in significant benefits in the form of reduced costs.

The benefit calculations are based on the following assumptions:

1. *Benefits noted in academic literature are assumed accurate and results were not externally validated.* Estimates of the benefits associated with the benefits are based on estimates obtained from the academic literature. Staff reviewed the academic articles for validity, but estimates were not replicated to confirm accuracy.

2. *Hospitals and eligible professionals that participate in the CMS EHR Incentive Program will be impacted.* Estimates are based on the assumption that 439,187 health care providers and/or 4,519 hospitals will be affected by this regulatory action.

3. *Estimates of the impact of real world testing on rates of interoperability (0.1 to 1%) are based on ONC analysis.* To identify the impact of real world testing on interoperability, we used regression analysis. Specifically, we estimated linear probability models that identified impact of 2014 Edition certified EHR on hospitals' interoperability (whether a hospital sends, receives, finds, and integrates summary of care records). Using data from the AHA from years 2014–2015 in the model, we controlled for hospital size, profit status, participation in a health information organization, and state and year fixed effects. The marginal effect of using a 2014 Edition was a five percentage point increase in interoperability. This is an upper bound estimate. For the purpose of this analysis, we assume 0.1% to 1% would be a reasonable range for real world testing to impact interoperability.

4. *Impact of real world testing is also based on the estimated number of providers that switch health IT developers (rate = 5%).* Using CMS Medicare EHR Incentive Program data from years 2013–2016, we estimate the rate of providers (hospitals and eligible professionals) that changed their health IT developer.

5. *Estimates of the rate of eligible professionals (10%) and hospitals (5%) that will be impacted by real world testing are based on ONC complaint data.* Because real world testing is designed to improve usability and interoperability of products, we assume that those eligible professionals and hospitals most likely to be impacted are those who currently use products by health IT developers with complaints.

As noted previously in this analysis, we acknowledge that there might be shared benefits across certain proposals and have taken steps to ensure that the benefits attributed to each proposal are unique to the proposal referenced. Specifically, we used regression analysis to calculate the impact of our real world testing and API proposals on interoperability. We assumed that the real world testing and API proposals would collectively have the same impact on interoperability as use of 2014 Edition certified health IT. Therefore, we estimated linear probability models that identified the impact of 2014 Edition certified health IT on hospitals' interoperability.[183] We controlled for additional factors such as participation in a health information exchange organization, hospital characteristics, and urban/rural status. We found the marginal effect of using 2014 Edition certified health IT was a five percentage point increase in interoperability.

While we acknowledge that there might be shared benefits across proposals, we have taken steps to ensure that the benefits attributed to each proposal is unique to the proposal referenced. We assumed that this marginal effect is true for our proposals and distributed the 5% benefit across our real world testing and API proposals at (.1–1%) to (1–4%) respectively. Moreover, the number of providers impacted is proposal specific. Given data limitations, we believe this approach allows us to estimate the benefits of our proposals without double counting the impact each proposal might have on interoperability.

The first table below shows benefits of real world testing for providers where we monetize the impact of real world testing as total amount saved by reducing provider time spent with the health IT. The impact of real world testing on provider time is expected to represent a larger impact (5%) than the impact of real world testing on health outcomes (1%–4%) and cost. This is primarily because provider behavior is more directly affected by improvements in interoperability.

Benefits of Real World Testing

TABLE 22—BENEFIT OF REAL WORLD TESTING FOR PROVIDERS

[2016 Dollars]

Benefit type	Number affected	Hourly wage	Hours saved (percent) [a] [b]		Hours per day with EHR	Number of working days in a year	Total benefit [c] (per year)	
			Min	Max			Min	Max
Reduction in provider time spent in health IT by improving usability and interoperability.	43,919 providers or 10% [d] (based on complaint data).	95	1	5	[e] 6	260	$65M	$325M
Administrative time spent in health IT by improving billing, patient matching, product integration.	Using a rule of 0.75 administrative staff per provider,[f] 32,939 personnel.	14.52	1	5	[e] 6	260	7M	37M

[183] American Hospital Association Health IT Supplement Survey, *http://www.ahadata.com/aha-healthcare-database/.*

TABLE 22—BENEFIT OF REAL WORLD TESTING FOR PROVIDERS—Continued

[2016 Dollars]

Benefit type	Number affected	Hourly wage	Hours saved (percent) [a b]		Hours per day with EHR	Number of working days in a year	Total benefit [c] (per year)	
			Min	Max			Min	Max
Number of providers switching health IT [g].	Number 2,195; Cost of Switching Min = $15,000, Max = $70,000.	....	....	....	....	....	33M	154M
Total Benefit	....	....	....	....	....	....	105M	516M

[a] Julia Adler-Milstein and Robert S. Huckman, *The Impact of Electronic Health Record Use on Physician Productivity,* Am J Manag Care (Nov. 19, 2013).

[b] Amusan, Tongen, Speedie, and Mellin, *A time-motion study to evaluate the impact of EMR and CPOE implementation on physician efficiency,* J. Healthcare Inf. Manag. (Fall 2008), at 31–7.

[c] Total benefits for the provider and administrative time spent in health IT by improving usability and interoperability. Total benefits from switching EHR vendor is a product of number providers switching and cost of EHR.

[d] The estimate is based on the number of providers that currently possess products with complaints. This is identified by flagging health IT developers and products about whom/which complaints are logged on ONC's database. These health IT developers are then matched to physicians using the Meaningful Use database.

[e] Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialtie*s, Ann Intern Med. (Dec. 6, 2016), at 753–60.

[f] Physician Practice, *Calculating the Right Number of Staff for Your Medical Practice, available at http://www.physicianspractice.com/blog/calculating-right-number-staff-your-medical-practice.*

[g] This estimate was obtained from Meaningful Use data from years 2013–2016. "Switching" is defined as an annual change in all health IT developers by providers/hospitals.

TABLE 23—BENEFIT OF REAL WORLD TESTING FOR PATIENTS AND PAYERS

[2016 Dollars]

Benefit type	Population affected	Overall interop impact (marginal effect)	Impact of real world testing		Total cost	Percent of total cost impacted	Total benefit [a] (per year)	
			Min	Max			Min	Max
Duplicate testing ...	35,607 providers ..	[b] 0.09	0.001	0.01	200 Billion [c]	10	$18M	$180M
Avoidable hospitalizations and readmissions.	5% of hospitals (n = 226).	[b] 0.09	0.001	0.01	$41B [d]	5	0.2M	1.8M
ER visits	5% of visits affected.	[b] 0.03	0.001	0.01	Cost per ER visit $1,233, 131M visits [e].	5	2M	2.4M
Adverse drug events.	5% of events affected.	[f] 0.22	0.001	0.01	$30 billion [g]	5	0.33M	3.3M
Total Benefit ..	....	....	....	....	....	....	2.6M	25.6M

[a] Total benefit is a product of *total cost, % of total cost impacted, overall impact of interoperability, and impact of real world testing.*

[b] Stephen E. Ross, Tiffany A. Radcliff, William G. Leblanc, L. Miriam Dickinson, Anne M. Libby, and Donald E. Nease Jr., Effects of health information exchange adoption on ambulatory testing rates, J. Am. Med. Inform. Assoc. (2013), at 1137–1142; Bridget A. Stewart, Susan Fernandes, Elizabeth Rodriguez-Huertas, and Michael Landzberg, A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients, J. of the Am. Med. Informatics Assoc. (2010), at 341–344; Sezgin Ayabakan, Indranil R. Bardhan, Zhiqiang (Eric) Zheng, and Kirk Kirksey Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals, MIS Quarterly (Jan. 1, 2017); Eric J. Lammers, Julia Adler-Milstein, and Keith E. Kocher, Does health information exchange reduce redundant imaging? Evidence from emergency departments, Med Care (Mar. 2014), at 227–34.

[c] National Academy of Medicine. (2016), *http://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html.*

[d] Agency for Healthcare Research and Quality (AHRQ) Statistical Brief #199 (Dec. 2015), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb199-Readmissions-Payer-Age.pdf;* AHRQ Statistical Brief #72, Nationwide Frequency and Costs of Potentially Preventable Hospitalizations (Apr. 2009), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb72.pdf.*

[e] National Center for Health Statistics (NCHS) Data Brief No. 252 (June 2016), *https://www.cdc.gov/nchs/data/databriefs/db252.pdf;* Nolan Caldwell, Tanja Srebotnjak, Tiffany Wang, and Renee Hsia, "How Much Will I Get Charged for This?" Patient Charges for Top Ten Diagnoses in the Emergency Department (2013), *https://doi.org/10.1371/journal.pone.0055491.*

[f] M.F. Furukawa, W.D. Spector, M.R. Limcangco, and W.E. Encinosa, *Meaningful use of health information technology and declines in in-hospital adverse drug events,* J. of the Am. Med. Informatics Assoc. (2017).

[g] Janet Sultana, Paola Cutroneo, and Gianluca Trifirò, *Clinical and economic burden of adverse drug reactions* (Dec. 2013).

Based on the stated assumptions and benefits outlined in Table 22 above, we estimate the total annual benefit for real world testing to providers would, on average, range from $105 million to $516 million. Based on the stated assumptions and benefits outlined in Table 23 above, we estimate the total annual benefit for patients and payers would, on average, range from $4.3 million to $25.5 million. Therefore, we estimate the total benefit of real world testing would, on average, range from $109.3 million to $541.5 million. If we assume, based on our cost estimates, the average annual costs to health IT developers would be $46 million and that increased health IT developer costs are passed to customers, then the net benefit to hospitals/providers would range from $63.3 million to $495.5 million.

We recognize that health IT developers may deploy their systems in a number of ways, including cloud-based deployments, and seek comment on whether our cost estimates of real world testing should factor in such methods of system deployment. For example, we request feedback about whether health IT developers would incur reduced real world testing costs through cloud-based deployments as opposed to other deployment methods. We specifically solicit comment on the general ratio of cloud-based to non-cloud-based deployments within the health care ecosystem and specific cost variations in performing real world testing based on the type of deployment. We also request comment on our assumptions about the burden to providers in time spent assisting health IT developers since we encourage health IT developers to come up with ways to perform real world testing that mitigate provider disruption.

3.6.1 Real World Testing Maintenance Requirements

We propose to revise the Principle of Proper Conduct in § 170.523(m) to require ONC–ACBs to collect, no less than quarterly, all updates successfully made to standards in certified health IT pursuant to the developers having opted to avail themselves of the Standards Version Advancement Process flexibility under the real world testing Condition of Certification. Under § 170.523(p), ONC–ACBs will be responsible for: (1) Reviewing and confirming that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1); (2) reviewing and confirming that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2); and (3) submitting real world testing plans by December 15 and results by April 1 of each calendar year to ONC for public availability. In addition, under § 170.523(t), ONC–ACBs will be required to: (1) Maintain a record of the date of issuance and the content of developers' notices; and (2) timely post content of each notice on the CHPL.

Using the information from the ''Real World Testing'' section of this RIA, we estimate that 429 developers will be impacted by real world testing. We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to collect all updates made to standards in Health IT Modules in accordance with § 170.523(m). The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Since the collection must occur no less than quarterly, we assume it occurs, on average, four times per year. Therefore, we estimate the annual cost to ONC–ACBs to comply with the collection requirements under § 170.523(m) to be $139,867.

We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 1 hour to review and confirm that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1). We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to review and confirm that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2). We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to submit real world testing plans and results to ONC for public availability. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate the annual cost to ONC–ACBs to comply with the submission and reporting requirements under §§ 170.523(m) and 170.550(l) to be $143,891.

Throughout the RIA we have used 830 products as our 2015 Edition Projection. We came up with this projection by multiplying a −23.2% market consolidation rate from the total number of products certified to 2014 Edition. This assumption was based on the market consolidation rate observed between the 2011 and 2014 Editions. We have estimated the number of 2015 Edition products that will certify each criteria included in the real world testing Condition of Certification. We assume that there will be a cost associated with a notice for each certified criteria (even if an individual product were to update the same standard across multiple criteria that use that standard). This estimation was calculated by multiplying the current percent of 2015 Edition products that certify a criteria by the estimated number of total 2015 Edition products (830).

We assume that the amount of time for an ONC–ACB staff person to (1) maintain a record of the date of issuance and the content of developers' notices; and (2) to timely post content of each notice on the CHPL can be anywhere from 30 minutes to 1 hour.

The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. This was the hourly rate we used for the RIA, so it's consistent with prior calculations. This wage is used to determine the ONC–ACB time cost to complete this requirement under § 170.523(t). Our minimum estimate for the amount of time to comply is 30 minutes per notice. If 25% of certified products update any of the applicable standards, we estimate it will cost $58,807. If all products update any of the applicable standards, we estimate it will cost $235,231. Our maximum estimate for the amount of time to comply is 1 hour per notice. If 25% of certified products update any of the applicable standards, we estimate it will cost $117,615. If all products update any of the applicable standards, we estimate it will cost $470,462. Our lower bound estimate for the cost of this requirement is $58,807. Our upper bound estimate for the cost of this requirement is $470,462.

3.8 Attestations

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, provide to the Secretary an attestation to all the Conditions and Maintenance of Certification specified in the Cures Act, except for the ''EHR reporting program'' Condition of Certification. It also requires that a health IT developer attest to ensuring that its health IT allows for health information to be exchanged, accessed, and used in the manner described by the API Condition of Certification. We propose to implement the Cures Act ''attestations'' Condition of Certification in § 170.406 by requiring health IT developers to attest to the aforementioned conditions. For the purposes of estimating the potential burden of these attestations on health IT developers, ONC–ACBs, and ONC, we are estimating that all health IT developers under the Program will submit an attestation biannually. As noted previously in this RIA, there are 792 health IT developers certified to the 2014 Edition.

We estimate it will take a health IT developer employee approximately one hour on average to prepare and submit each attestation to the ONC–ACB. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a software developer is $50.14 [184] Therefore, we estimate the annual cost including overhead costs to be $79,422.

We propose that attestations would be submitted to ONC–ACBs on behalf of ONC and the Secretary. We assume there will be three ONC–ACBs as this is the current number of ONC–ACBs, and we also assume an equal distribution in responsibilities among ONC–ACBs. ONC–ACBs would have two responsibilities related to attestations. One responsibility we propose in § 170.523(q) is that an ONC–ACB must review and submit the health IT developers' attestations to ONC. We estimate it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes on average to review and submit each attestation to ONC. The other responsibility we propose in § 170.550(l) is that before issuing a certification, an ONC–ACB would need to ensure that the health IT developer of the Health IT Module has met its responsibilities related to the Conditions and Maintenance of Certification requirements as solely evidenced by its attestation. We estimate it will take an ONC–ACB

[184] *See https://www.bls.gov/oes/2016/may/oes439061.htm.*

employee at the GS–13, Step 1 level approximately one hour on average to complete this task. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate the annual cost to ONC–ACBs to be $209,801.

We propose that ONC would make the attestations publicly available on the CHPL once they are submitted by the ONC–ACBs. ONC posts information regularly to the CHPL and we estimate the added costs to post the attestation will be de minimis. We welcome comments if stakeholders believe more or less networks should be included in our estimate.

(4) Oversight for the Conditions and Maintenance of Certification

ONC's processes for overseeing the Conditions and Maintenance of Certification will, for the most part, mirror ONC's processes for direct review of non-conformities in certified health IT as described in current § 170.580. We have proposed that ONC may directly review a health IT developer's actions to determine whether they conform to the Conditions and Maintenance of Certification requirements proposed in this proposed rule. The estimated costs and benefits for such oversight and review are detailed below.

Costs

We estimated the potential monetary costs of our proposal to allow ONC to directly review a health IT developer's actions to determine whether the actions conform to the requirements of the Program as follows: (1) Costs for health IT developers to correct non-conforming actions identified by ONC; (2) costs for health IT developers and ONC related to ONC review and inquiry into non-conforming actions by the health IT developer; and (3) costs for ONC–ACBs related to the new proposed reporting requirement in the Principles of Proper Conduct in § 170.523(s).

Costs for Health IT Developers To Correct Non-Conforming Actions Identified by ONC

We do not believe health IT developers face additional direct costs for the proposed ONC direct review of health IT developer actions (*see* cost estimates for the Conditions and Maintenance of Certification requirements). However, we acknowledge that this proposed rule may eventually require health IT developers to correct certain actions or non-conformities with their health IT that do not conform to the Conditions and Maintenance of Certification.

If ONC identifies a non-conforming action by a health IT developer, the costs incurred by the health IT developer to bring its actions into conformance would be determined on a case-by-case basis. Factors that would be considered include, but are not limited to: (1) The extent of customers and/or business affected; (2) how pervasive the action(s) is across the health IT developer's business; (3) the period of time that the health IT developer was taking the action(s) in question; and (4) the corrective action required to resolve the issue. We are unable to reliably estimate these costs as we do not have cost estimates for a comparable situation. We request comment on existing relevant data and methods we could use to estimate these costs.

Costs for Health IT Developers and ONC Related to ONC Review and Inquiry Into Health IT Developer Actions

In order to calculate the potential costs to health IT developers and ONC related to ONC review and inquiry into health IT developer actions, we have created the following categories for potential costs: (1) ONC review and inquiry prior to the issuance of a notice of non-conformity; (2) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer does not contest ONC's findings (*i.e.,* no appeal); and (3) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer contests ONC's findings (*i.e.,* appeal).

ONC Review and Inquiry Prior to the Issuance of a Notice of Non-Conformity

We anticipate that ONC will receive, on average, between 100 and 200 complaints per year concerning the Conditions and Maintenance of Certification that will warrant review and inquiry by ONC. We estimate that such initial review and inquiry by ONC would require, on average, two to three analysts at the GS–13 level working one to two hours each per complaint. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Therefore, we estimate each review and inquiry would cost ONC, on average, between $177 and $529. We estimate the total annual cost to ONC would, on average, range from $17,700 and $105,800. This range takes into account both the low end of reviews that are resolved quickly and the high end in which staff would need to discuss issues with ONC leadership or in some cases, HHS senior leadership including the Office of General Counsel. We have not estimated health IT developer costs associated with ONC review prior to the issuance of a notice of non-conformity because, in most cases, health IT developers are not required to take action prior to the notice of non-conformity.

ONC Review and Inquiry Following the Issuance of a Notice of Non-Conformity and the Health IT Developer Does Not Contest ONC's Findings

This category would capture cases that require review and inquiry following ONC's issuance of a notice of non-conformity, but that would not proceed to the appeals process. Examples of such situations would include, but not be limited to: (1) A health IT developer violates a Condition of Certification and does not contest ONC's finding that it is in violation of the Condition of Certification; or (2) a health IT developer fails to meet a deadline, such as for its corrective action plan (CAP). We estimate that ONC will, on average, conduct between 12 and 18 of these reviews annually.

We estimate that a health IT developer may commit, on average and depending on complexity, between 10 and 40 hours of staff time per case to provide ONC with all requested records and documentation that ONC would use to review and conduct an inquiry into health IT developer actions, and, when necessary, make a certification ban and/or termination determination. We assumed that the work would be performed by a ''Computer Systems Analyst.'' According to the May 2016 BLS occupational employment statistics, the mean hourly wage for computer systems analyst is $44.05.[185] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100% of pre-tax wages, so the hourly wage including overhead costs would be $88.10. Therefore, we estimate the average annual cost for health IT developers would range from $10,572 to $63,432. We note that some health IT developers' costs are expected to be less and some health IT developers' costs are expected to be more than this estimated cost range. Further, we note that these costs would be perpetual.

We estimate that ONC may commit, on average and depending on complexity, between 8 and 80 hours of staff time to complete a review and inquiry into health IT developer actions. We assume that the expertise of a GS–15, Step 1 federal employee(s) would be

[185] *https://www.bls.gov/oes/2016/may/oes439061.htm.*

necessary. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, based on the estimate of between 12 and 18 cases each year, we estimate ONC's annual costs would on, average range, from $11,783 to $176,745. We note that some reviews and inquiries may cost less and some may cost more than this estimated cost range. Further, we note that these costs would be perpetual.

We welcome comments on our estimated costs and any comparable processes and costs that we could use to improve our cost estimates.

ONC Review and Inquiry Following the Issuance of a Notice of Non-Conformity and the Health IT Developer Contests ONC's Findings

As discussed in section VII.C of this preamble, we propose to permit a health IT developer to appeal an ONC determination to issue a certification ban and/or terminate a certification under § 170.581(a)(2)(iii). This category of cost calculations captures cases that require review and inquiry following ONC's issuance of a notice of non-conformity and where the health IT developer contests ONC's finding and files an appeal. We estimate that ONC will, on average, conduct between three and five of these reviews annually.

We estimate that a ''Computer Systems Analyst'' for the health IT developer may commit, on average and depending on complexity, between 20 and 80 hours to provide the required information to appeal a certification ban and/or termination under § 170.581(a)(2)(iii) and respond to any requests from the hearing officer. According to the May 2016 BLS occupational employment statistics, the mean hourly wage for a computer systems analyst is $44.05.[186] Assuming that overhead costs (including benefits) are equal to 100% of pre-tax wages, the hourly wage including overhead costs is $88.10. Therefore, we estimate the annual cost, including overhead costs, for a health IT developer to appeal a certification ban and/or termination under § 170.581(a)(2)(iii) would, on average, range from $5,286 to $35,240. We note that some health IT developers' costs are expected to be less and some health IT developers' costs are expected to be more than this estimated cost range. Further, we note that these costs would be perpetual.

We estimate that ONC would commit, on average and depending on complexity, between 40 and 160 hours of staff time to conduct each appeal. This would include the time to represent ONC in the appeal and support the costs for the hearing officer. We assume that the expertise of a GS–15, Step 1 federal employee(s) would be necessary. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, based on the estimate on between three and five cases each year, we estimate the cost for ONC to conduct an appeal would, on average, range from $14,729 to $98,192. We note that some appeals may cost less and some may cost more than this estimated cost range. Further, we note that these costs would be perpetual.

Based on the above estimates, we estimate the total annual costs for health IT developers related to ONC review and inquiry into health IT developer actions would, on average, range from $15,858 to $98,672. We estimate the total annual costs for ONC related to ONC review and inquiry into health IT developer actions would, on average, range from $44,212 to $380,737.

We welcome comments on our estimated costs and any comparable processes and costs that we could use to improve our cost estimates.

Costs for ONC–ACBs

We also note that ONC–ACBs could realize costs associated with the new proposed reporting requirement in the Principles of Proper Conduct in § 170.523(s) that they report, at a minimum, on a weekly basis to the National Coordinator any circumstances that could trigger ONC direct review per § 170.580(a)(2). We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to prepare the report. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $88.30. Since the collection must occur no less than weekly, we will assume it occurs, on average, 52 times per year. Therefore, given that there are currently three ONC–ACBs, we estimate the annual cost to ONC–ACBs to comply with the reporting requirement under § 170.523(s) would, on average, be $6,889.

Benefits

This proposed rule's provisions for ONC direct review of the Conditions and Maintenance of Certification requirements would promote health IT developers' accountability for their actions and ensure that health IT developers' actions conform with the requirements of the Cures Act and Conditions and Maintenance of Certification requirements in §§ 170.400–406. Specifically, ONC's direct review of health IT developer actions will facilitate ONC's ability to require comprehensive corrective action by health IT developers to address non-conforming actions determined by ONC. If ONC ultimately implements a certification ban and/or terminates a certification(s), such action will serve to protect the integrity of the Program and users of health IT. While we do not have available means to quantify the benefits of ONC direct review of health IT developer actions, we note that ONC direct review supports and enables the National Coordinator to fulfill his responsibilities under the HITECH Act and Cures Act, instills public confidence in the Program, and protects public health and safety.

(5) Information Blocking

Costs

We expect ONC to incur an annual cost for issuing guidance related to the information blocking ''reasonable and necessary'' exceptions. We assume that the guidance would be provided by ONC staff with the expertise of a GS–15, Step 1 federal employee(s). The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. We estimate it would take ONC staff between 200 and 400 hours to develop the guidance. Therefore, we estimate the annual cost to ONC would, on average, range from $98,192 to $196,384.

Benefits

Information blocking not only interferes with effective health information exchange, but also negatively impacts many important aspects of health and health care. To make informed health care decisions, providers and individuals must have timely access to information in a form that is usable. When health information is unavailable, decisions can be impaired—and so too the safety, quality, and effectiveness of care provided to patients. Information blocking impedes progress towards reforming health care delivery and payment because sharing information seamlessly across the care continuum is fundamental to moving to a person-centered, high-performing health care system. Information blocking can undermine consumers' confidence in their health care providers by preventing individuals from accessing their health information and using it to make informed decisions

[186] *See https://www.bls.gov/oes/2016/may/oes439061.htm. https://www.bls.gov/oes/2016/may/oes439061.htm.*

about their health and health care. Information blocking also prevents advances in biomedical and public health research, which require the ability to analyze information from many sources in order to identify public health risks, develop new treatments and cures, and enable precision medicine.

In addition, information blocking is a practice that is profoundly anti-consumer and anti-competition. Information blocking can be used to increase revenue, escalate prices, and prevent market competition both for current and future competitors and for new services. For instance, a study released in 2017 about the prevalence of information blocking and how to address it assessed the perceived motivations for information blocking. The study found that respondents perceived that information-blocking practices by health IT developers were often motivated by a desire to maximize short-term revenue and to increase the likelihood that providers will select their health IT instead of a competitor's health IT. Among hospitals and health systems, the most frequent perceived motivation was also related to improving revenue, namely to strengthen their competitive position in the market, followed by accommodating more important internal priorities than health information exchange.[187]

According to leaders of health information exchange efforts, information blocking is relatively widespread.[188] Half of leaders of health information exchange efforts (n = 60) nationwide reported that they routinely encountered information blocking by health IT developers. The top three types of information blocking practices they encountered on a routine basis included:

- Deployment of products with limited interoperability (49%);
- High fees for health information exchange unrelated to cost (47%); and
- Making third-party access to standardized data difficult (42%).

Many hospitals have experienced the negative impacts of health IT developer information blocking practices. In 2015, almost half of hospitals (46%) nationwide reported difficulty exchanging data with providers whose health IT system differed from theirs and one-quarter of hospitals reported paying additional costs to exchange electronic health information with providers outside their hospital system.[189] There is also emerging evidence related to the negative impacts of information blocking at the market level on hospitals' health information exchange activity.[190] Health information exchange activity among hospitals who are using a dominant health IT developer within a given hospital referral region was found to be significantly higher compared to those that are using a non-dominant health IT developer, particularly in more competitive markets where dominant health IT developers had a smaller share of the market. As information blocking diminishes and information blocking becomes less prevalent, such gaps in rates of exchange and barriers to exchange of health information should diminish. Considering the above motivations for and consequences of information blocking, we believe health care providers and patients will benefit greatly from compliance with the information blocking definition. Our proposal would promote the free flow of electronic health information when and where it is needed.

We have also included provisions in this proposed rule that would establish exceptions to the definition of information blocking, which we estimate will generate significant net benefits. As noted above, section 3022 of the PHSA defines information blocking broadly section 3022(a)(3) instructs authorizes the Secretary to identify reasonable and necessary activities that would be considered establish exceptions to the definition of information blocking. In this rule, we propose to establish several exceptions. The exceptions, if finalized, would create clear guidelines for industry regarding pro-competitive and other beneficial activities and would enable stakeholders to determine more easily and with greater certainty whether their activities are excepted from the information blocking definition. The additional clarity provided by the exceptions would make it easier for these regulated entities to comply with the statute—resulting in reduced compliance costs—and would result in increased predictability, which would allow regulated entities to more effectively plan and invest resources in developing and using interoperable technologies and services to improve health care efficiency and value. Overall, the proposed exceptions are accommodating to legitimate industry practices for health IT developers, hospitals, and health care providers and, we believe, would ease the burden and compliance costs for these parties.

Due to limited data and research available, we have only estimated the benefits of our information blocking proposals for payers, specifically patients and insurers. In order to quantify the magnitude of information blocking and the benefits of restricting information blocking, we estimated the following expression, which gives us the imposed cost of information blocking for each health outcome: [% providers that engage in cross-vendor exchange] × [marginal effect (ME) of information blocking] × [ME effect of interoperability] × [total cost of health outcome].

We extracted the ''ME effect of interoperability'' and ''cost of health outcomes'' from academic literature (*see* citations in Table 24). We used a proxy of the ''percent of providers engaged in cross-vendor exchange'' with the ''percent of hospitals engaged in cross-vendor referral of patients outside their system'' (82% in 2015).

We estimated the ''ME of information blocking'' through the following research design. We looked at hospitals that switched vendors and examined their referral patterns before and after the switch. If hospitals that switched vendors also had to change their referral patterns, this could be evidence of information blocking. To operationalize this experiment, we estimated the following equation:

$Y = b * S + r + h + e.$

In this equation, the variables are as follows:

- Y = Percent of referrals to providers using a vendor to which the hospital switched
- b = Estimate of interest, which reflects the change in referral to the vendors after the switch relative to hospitals that did not switch. After controlling for hospital and year fixed, this is essentially an interaction effect of the year with the switch.
- S = Indicator for whether hospital switched vendor
- r = Year
- h = Hospital fixed effects
- e = Error term (every regression has an error term)

We used CMS referral data and linked it with Healthcare Information and Management Systems Society (HIMSS) and AHA data for information on hospitals' vendors and other characteristics. Our estimate for ''b'' is 0.4 percentage points, meaning if a

[187] Julia Adler-Milstein and Eric Pfeifer, *Information Blocking: Is It Occurring And What Policy Strategies Can Address It?,* 95 Milbank Quarterly 117 (Mar. 2017) at 124–5, *available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full.*

[188] *Id.*

[189] Vaishali Patel, JaWanna Henry, Yuriy Pylypchuk, and Talisha Searcy, Interoperability among U.S. Non-federal Acute Care Hospitals in 2015, ONC Data Brief, No.36 (May 2016).

[190] Jordan Everson and Julia Adler-Milstein, *Engagement In Hospital Health Information Exchange Is Associated With Vendor Marketplace Dominance,* Health Affairs. 35, No. 7 (2016), at 1286–93.

hospital switches to vendor X, the referrals to hospitals with that vendor increases by a rate of 0.4 percentage points. This number we interpret as a proxy for the extent to which difficulties in cross vendor exchange hinder patient care. However, our finding does not imply that difficulties in cross vendor exchange can be entirely attributed to information blocking. One source of difficulties could be explained by technological challenges where inherent software differences among vendors hinder cross vendor exchange. An additional reason for this result could be attributed to contractual agreements where vendors may incentivize their clients to exchange with other clients having the same vendor. Nevertheless, to keep our estimates conservative, we reduced our estimates by a factor of five. Hence, we use 0.08 percentage points as the ''ME of information blocking.''

Our estimates are detailed in the table below.

TABLE 24—BENEFITS OF PROHIBITING AND/OR DETERRING INFORMATION BLOCKING

[2016 Dollars]

Benefit type	Percent of total cost impacted	Total cost	Overall interop impact (marginal effect)	Percent of providers susceptible to information blocking	Marginal effect of information blocking	Benefit [a]
Duplicate testing	100	200 Billion [b]	[c] 0.09	82	0.08	$1.1B
Avoidable hospitalizations and readmissions.	100	$41B [d]	0.09	82	0.08	242M
ER visits	100	Cost per ER visit $1,233, 131M visits [e].	0.03	82	0.08	317M
Adverse drug events	100	$30 billion [f]	0.22	82	0.08	86M
Total benefit per year						1.8B

[a] Total benefit is a product of *% of total cost impacted, total cost, overall interop impact, percent of providers susceptible to information blocking, and marginal effect of information blocking.*

[b] National Academy of Medicine (2016), *http://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html.*

[c] Stephen E. Ross, Tiffany A. Radcliff, William G. Leblanc, L. Miriam Dickinson, Anne M. Libby, and Donald E. Nease Jr., *Effects of health information exchange adoption on ambulatory testing rates,* J. Am. Med. Inform. Assoc. (2013), at 1137–1142; Bridget A. Stewart, Susan Fernandes, Elizabeth Rodriguez-Huertas, and Michael Landzberg, *A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients,* J. of the Am. Med. Informatics Assoc. (2010), at 341–344; Sezgin Ayabakan, Indranil R. Bardhan, Zhiqiang (Eric) Zheng, and Kirk Kirksey *Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals,* MIS Quarterly (Jan. 1, 2017); Eric J. Lammers, Julia Adler-Milstein, and Keith E. Kocher, *Does health information exchange reduce redundant imaging? Evidence from emergency departments,* Med Care (Mar. 2014), at 227–34.

[d] Agency for Healthcare Research and Quality (AHRQ) Statistical Brief #199 (Dec. 2015), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb199-Readmissions-Payer-Age.pdf;* AHRQ Statistical Brief #72, Nationwide Frequency and Costs of Potentially Preventable Hospitalizations (Apr. 2009), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb72.pdf.*

[e] National Center for Health Statistics (NCHS) Data Brief No. 252 (June 2016), *https://www.cdc.gov/nchs/data/databriefs/db252.pdf;* Nolan Caldwell, Tanja Srebotnjak, Tiffany Wang, and Renee Hsia, ''How Much Will I Get Charged for This?'' Patient Charges for Top Ten Diagnoses in the Emergency Department (2013), *https://doi.org/10.1371/journal.pone.0055491.*

[f] Janet Sultana, Paola Cutroneo, and Gianluca Trifirò, *Clinical and economic burden of adverse drug reactions.*

We request comment on our approach to estimating these benefits, as well as the benefit estimates in the table above.

(6) Total Annual Cost Estimate

We estimate that the total annual cost for this proposed rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would, on average, range from $365 million to $919 million with an average annual cost of $642 million. We estimate that the total perpetual cost for this proposed rule (starting in year two), based on the cost estimates outlined above, would, on average, range from $228 million to $452 million with an average annual cost of $340 million. We also include estimates based on the stakeholder group affected. We estimate the total costs to health IT developers to be between $373 million and $933 million (including one-time and perpetual costs) with $569,000 in cost savings. We estimate the total costs to ONC–ACBs to be between $213,000 and $311,000. We estimate the government (ONC) costs to be between $44,800 and $269,000 while saving $4,500. In addition, to the above mentioned cost savings that are attributable to specific stakeholder groups, we estimate to an additional cost savings of $6.8 million to $13.7 million to all stakeholders affected by this proposal. We are unable to attribute these amounts to specific stakeholder groups.

(7) Total Annual Benefit Estimate

We estimate the total annual benefit for this proposed rule, based on the benefit estimates outlined above, would range from $3.08 billion to $9.15 billion with an average annual benefit of $6.1 billion. We attribute between $756 million and $3.8 billion in benefits to hospitals and clinicians. We attribute between $2.1 billion and $2.9 billion to payers and patients. Our estimates include benefits attributed to the whole health care system, not just to the stakeholders mentioned above.

(8) Total Annual Net Benefit

We estimate the total annual net benefit for this proposed rule for the first year after it is finalized (including one-time costs), based on the estimates outlined above, would range from $2.7 billion to $8.2 billion with an average net benefit of $5.5 billion. We estimate the total perpetual annual net benefit for this proposed rule (starting in year two), based on the estimates outlined above, would range from $2.9 billion to $8.7 billion with an average net benefit of $5.8 billion.

b. Accounting Statement and Table

When a rule is considered an economically significant rule under Executive Order 12866, we are required to develop an accounting statement indicating the classification of the expenditures associated with the provisions of the proposed rule. Monetary annual benefits are presented as discounted flows using 3% and 7% factors in Table 25 below. We are not able to explicitly define the universe of all costs, but have provided an average of likely costs of this proposed rule as well as a high and low range of likely costs. This proposed rule requires no federal annual monetized transfers.

TABLE 25—E.O. 12866 SUMMARY TABLE

[In $ millions, 2016 time period]

	Primary (3%)	Lower bound (3%)	Upper bound (3%)	Primary (7%)	Lower bound (7%)	Upper bound (7%)
Present Value of Quantified Costs	1,557	1,043	2,070	1,394	934	1,853
Non-quantified Costs	Text					
Present Value of Quantified Benefits	27,998	14,100	41,896	25,067	12,624	37,509
Non-quantified Benefits	Text					
Present Value of Net Benefits	2,456	1,129	37,620	2,190	1,011	33,681
Annualized Quantified Costs	330	355	433	318	365	422
Non-quantified Costs	Text					
Annualized Quantified Benefits	5,935	2,989	8,881	5,714	2,878	8,550
Non-quantified Benefits	Text					
Annualized Net Quantified Benefits	5,184	2,304	7,975	4,991	2,838	8,128

TABLE 26—E.O. 12866 SUMMARY TABLE NON-DISCOUNTED FLOWS

[2016 Dollars]

	Year 1	Year 2	Year 3	Year 4	Year 5
Costs	$641,853,087	$339,870,993	$339,870,993	$339,870,993	$339,870,993
Net Benefits	5,471,742,914	5,773,725,008	5,773,725,008	5,773,725,008	5,773,725,008
	Year 6	**Year 7**	**Year 8**	**Year 9**	**Year 10**
Costs	$339,870,993	$339,870,993	$339,870,993	$339,870,993	$339,870,993
Net Benefits	5,773,725,008	5,773,725,008	5,773,725,008	5,773,725,008	5,773,725,008

3. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. The Small Business Administration (SBA) establishes the size of small businesses for federal government programs based on average annual receipts or the average employment of a firm.[191] The entities that are likely to be directly affected by the requirements in this proposed rule requirements are health IT developers. We note that the proposed reasonable and necessary activities that do not constitute information blocking provide flexibilities and relief for health IT developers of certified health IT, health information networks, health information exchanges, and health care providers in relation to the information blocking provision of the Cures Act. These proposed reasonable and necessary activities also take into account the potential burden on small entities to meet these ''exceptions'' to information blocking, such as with considering the size and resources of small entities when meeting security requirements to qualify for the ''promoting the security of electronic health information'' exception. We refer readers to section VIII for our information blocking-related proposals and welcome comments on their impacts on small entities.

While health IT developers that pursue certification of their health IT under the Program represent a small segment of the overall information technology industry, we believe that many health IT developers impacted by the requirements proposed in this proposed rule most likely fall under the North American Industry Classification System (NAICS) code 541511 ''Custom Computer Programming Services.''[192] The SBA size standard associated with this NAICS code is set at $27.5 million annual receipts or less. There is enough data generally available to establish that between 75% and 90% of entities that are categorized under the NAICS code 541511 are under the SBA size standard. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification of their health IT under the Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it is difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not perfectly correlated to the size standard for NAICS code 541511, we do have information indicating that over 60% of health IT developers that have had Complete EHRs and/or Health IT Modules certified to the 2011 Edition have less than 51 employees.

We estimate that the proposed requirements in this proposed rule would have effects on health IT developers, some of which may be small entities, that have certified health IT or are likely to pursue certification of their health IT under the Program. We believe, however, that we have proposed the minimum amount of requirements necessary to accomplish our primary policy goal of enhancing interoperability. Further, as discussed in section XIV.B of this RIA above, there are no appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this proposed

[191] The SBA references that annual receipts means ''total income'' (or in the case of a sole proprietorship, ''gross income'') plus ''cost of goods sold'' as these terms are defined and reported on Internal Revenue Service tax return forms.

[192] *https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2017.pdf. https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2017.pdf.*

rule because many of the proposals are derived directly form legislative mandates in the Cures Act. Additionally, we have attempted to offset some of the burden imposed on health IT developers in this proposed rule with cost saving proposals through deregulatory actions (*see* proposed section III).

We do not believe that the proposed requirements of this proposed rule would create a significant impact on a substantial number of small entities, but request comment on whether there are small entities that we have not identified that may be affected in a significant way by this proposed rule. Additionally, the Secretary proposes to certify that this proposed rule would not have a significant impact on a substantial number of small entities.

4. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. Nothing in this proposed rule imposes substantial direct compliance costs on state and local governments, preempts state law, or otherwise has federalism implications. We are not aware of any state laws or regulations that are contradicted or impeded by any of the proposals in this proposed rule. We welcome comments on this assessment.

5. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule that imposes unfunded mandates on state, local, and tribal governments or the private sector requiring spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory threshold is approximately $150 million. While the estimated potential cost effects of this proposed rule reach the statutory threshold, we do not believe this proposed rule imposes unfunded mandates on state, local, and tribal governments or the private sector. We welcome comments on these conclusions.

6. Executive Order 13771 Reducing Regulation and Controlling Regulatory Costs

Executive Order 13771 (January 30, 2017) requires that the costs associated with significant new regulations ''to the extent permitted by law, be offset by the elimination of existing costs associated with at least two prior regulations.'' The Department believes that this rule is a significant regulatory action as defined by Executive Order 12866 which imposes costs, and therefore is considered a regulatory action under Executive Order 13771. The Department estimates that this rule generates $275 million in annualized costs at a 7% discount rate, discounted relative to 2016, over a perpetual time horizon.

OMB reviewed this proposed rule.

List of Subjects

45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and recordkeeping requirements, Public health, Security.

45 CFR Part 171

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health care provider, Health information exchange, Health information technology, Health information network, Health insurance, Health records, Hospitals, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter D, is proposed to be amended as follows:

PART 170—HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

■ 1. The authority citation for part 170 continues to read as follows:

Authority: 42 U.S.C. 300jj–11; 42 U.S.C 300jj–14; 5 U.S.C. 552.

■ 2. Revise § 170.101 to read as follows:

§ 170.101 Applicability.

The standards, implementation specifications, and certification criteria adopted in this part apply to Health IT Modules and the testing and certification of such Health IT Modules.

■ 3. Amend § 170.102 as follows:

■ a. Remove the definitions of ''2014 Edition Base EHR'', and ''2014 Edition EHR certification criteria'';

■ b. Amend the definition of ''2015 Edition Base EHR'' by revising paragraph (3);

■ c. Add, in alphabetical order, the definitions for ''API Data Provider'', ''API Technology Supplier'', and ''API User'';

■ d. Remove the definitions of ''Common Clinical Data Set'', and ''Complete EHR, 2014 Edition''; and

■ e. Add, in alphabetical order, the definitions for ''Fee'', ''Interoperability'', and ''Interoperability element''.

The revisions and additions read as follows:

§ 170.102 Definitions.

* * * * *

2015 Edition Base EHR * * *

(3) Has been certified to the certification criteria adopted by the Secretary in—

(i) Section 170.315(a)(1), (2), or (3); (5); (9); (14); (b)(1); (c)(1); (g)(7) and (9); and (h)(1) or (2);

(ii) Section 170.315(g)(8) or (10) until [24 months from the final rule's effective date]; and

(iii) Section 170.315(b)(10) and (g)(10) on and after [24 months from the final rule's effective date].

* * * * *

API Data Provider refers to the organization that deploys the API technology created by the ''API Technology Supplier'' and provides access via the API technology to data it produces and electronically manages. In some cases, the API Data Provider may contract with the API Technology Supplier to perform the API deployment service on its behalf. However, in such circumstances, the API Data Provider retains control of what and how information is disclosed and so for the purposes of this definition is considered to be the entity that deploys the API technology.

API Technology Supplier refers to a health IT developer that creates the API technology that is presented for testing and certification to any of the certification criteria adopted or proposed for adoption at § 170.315(g)(7) through (11).

API User refers to persons and entities that use or create software applications that interact with the APIs developed by the ''API Technology Supplier'' and deployed by the ''API Data Provider.'' An API User includes, but is not limited to, third-party software developers, developers of software applications used by API Data Providers, and patients and health care providers that use apps that connect to API technology on their behalf.

* * * * *

Fee is defined as it is in § 171.102 of this subchapter.

* * * * *

Interoperability is, with respect to health information technology, such health information technology that—

(i) Enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;

(ii) Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and

(iii) Does not constitute information blocking as defined in § 171.103 of this subchapter.

Interoperability element is defined as it is in § 171.102 of this subchapter.

* * * * *

§ 170.200 [Amended]

■ 4. Amend § 170.200 by removing the phrase ''Complete EHRs and.''

§ 170.202 [Amended]

■ 5. Amend § 170.202 by removing and reserving paragraph (a)(1).

§ 170.204 [Amended]

■ 6. Amend § 170.204 by removing and reserving paragraphs (b)(1) and (2), and by removing paragraph (c).

■ 7. Amend § 170.205 as follows:

■ a. Remove and reserve paragraphs (a)(1) and (2);

■ b. Add paragraph (a)(4)(i) and add and reserve paragraph (a)(4)(ii);

■ c. Add paragraph (b)(1);

■ d. Remove and reserve paragraphs (d)(2), (d)(3), (e)(3), (h)(1), (i)(1), and (j); and

■ e. Add paragraphs (h)(3) and (k)(3).

The revisions read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

(a) * * *

(4) * * *

(i) *Standard.* HL7 CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes R1 Companion Guide, Release 1 (incorporated by reference in § 170.299).

(ii) [Reserved]

* * * * *

(b) * * *

(1) *Standard.* National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 (incorporated by reference in § 170.299).

* * * * *

(h) * * *

(3) CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting Implementation Guide for 2019 (incorporated by reference in § 170.299).

* * * * *

(k) * * *

(3) CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2019 (incorporated by reference in § 170.299).

* * * * *

§ 170.207 [Amended]

■ 8. Amend § 170.207 by removing and reserving paragraphs (d)(2), (e)(2), (g)(1), (h), and (j).

§ 170.210 [Amended]

■ 9. Amend § 170.210 by removing and reserving paragraphs (a)(1) and (c)(1).

■ 10. Add § 170.213 to read as follows:

§ 170.213 United States Core Data for Interoperability

Standard. United States Core Data for Interoperability (USCDI), Version 1 (v1) (incorporated by reference in § 170.299).

■ 11. Add § 170.215 to read as follows:

§ 170.215 Application Programming Interface Standards.

The Secretary adopts the following application programming interface (API) standards and associated implementation specifications:

(a)(1) *Standard.* HL7 Fast Healthcare Interoperability Resources (FHIR) Draft Standard for Trial Use (DSTU) 2 (v1.0.2–7202) (incorporated by reference in § 170.299).

(2) *Implementation specifications. API Resource Collection in Health (ARCH) Version 1* (incorporated by reference in § 170.299).

(3) *Implementation specifications—FHIR profiles.* Argonaut Data Query Implementation Guide Version 1.0.0 (incorporated by reference in § 170.299).

(4) *Implementation specifications—FHIR server conformance.* Argonaut Data Query Implementation Guide Server (incorporated by reference in § 170.299).

(5) *Implementation specification—Application authorization. HL7* SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for ''refresh tokens,'' ''Standalone Launch,'' and ''EHR Launch'' requirements (incorporated by reference in § 170.299).

(b) *Application authentication. Standard.* OpenID Connect Core 1.0 incorporating errata set 1 (incorporated by reference in § 170.299).

(c)(1) *Standard.* HL7 Fast Healthcare Interoperability Resources (FHIR) Release 3 Standard for Trial Use (STU) 3 (v3.0.1) (incorporated by reference in § 170.299).

(2) *Implementation specification—FHIR consent resources. HL7* Consent2Share FHIR Consent Profile Design (incorporated by reference in § 170.299).

■ 12. Amend § 170.299 as follows:

■ a. Remove and reserve paragraphs (c)(2), (3), (d)(2), (7), and (8);

■ b. Add paragraphs (e)(4) and (5);

■ c. Remove and reserve paragraphs (f)(3), (6), (7), (10), and (11);

■ d. Add paragraphs (f)(30) through (36);

■ e. Redesignate paragraphs (o) through (r) and (g) through (n) as paragraphs (q) through (t) and (h) through (o), respectively;

■ f. Add new paragraph (g) and paragraph (i)(4);

■ g. Remove and reserve newly redesignated paragraph (k)(1);

■ h. Add paragraph (l)(3);

■ i. Remove and reserve newly redesignated paragraph (m)(3);

■ j. Add paragraphs (n)(5) and (6);

■ k. Add new paragraph (p); and

■ l. Remove and reserve newly redesignated paragraphs (s)(4), and (5).

The additions and revisions read as follows:

§ 170.299 Incorporation by reference.

* * * * *

(e) * * *

(4) CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting Implementation Guide for 2019, May 4, 2018, IBR approved for § 170.205(h).

(5) CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2019, October 8, 2018, IBR approved for § 170.205(k).

(f) * * *

(30) HL7 CDA Release 2 Implementation Guide: C–CDA Templates for Clinical Notes R1 Companion Guide, Release 1, March 2017, IBR approved for § 170.205(a).

(31) HL7 Fast Healthcare Interoperability Resources (FHIR®) Release 2.0, Draft Standard for Trial Use (DSTU) Version 1.0.2–7202, October 24, 2015, IBR approved for § 170.215(a).

(32) HL7 Fast Healthcare Interoperability Resource Specification (FHIR®) Release 3 Standard for Trial Use (STU), Version 3.0.1, February 21, 2017, IBR approved for § 170.215(c).

(33) HL7 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, Version 4.0.0,

December 27, 2018, IBR approved for § 170.215.

(34) HL7 Implementation Specification—FHIR Profile: Consent2Share FHIR Consent Profile Design, December 11, 2017, IBR approved for § 170.215(c).

(35) HL7 CDA R2 Implementation Guide: C–CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1—US Realm, November 15, 2018, IBR approved for § 170.205.

(36) HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0, November 13, 2018, IBR approved for § 170.215(a).

(g) HL7® FHIR® Foundation. 3300 Washtenaw Avenue, Suite 227, Ann Arbor, MI 48104; Telephone (734) 677–7777 or *https://www.fhir.org/.*

(1) Argonaut Data Query Implementation Guide. Version 1.0.0, December 23, 2016, IBR approved for § 170.215(a).

(2) Argonaut Data Query Implementation Guide Server, Version 1.0.2, December 15, 2016, IBR approved for § 170.215(a).

* * * * *

(i) * * *

(4) OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591), July 2015, IBR approved for § 170.215.

* * * * *

(l) * * *

(3) National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 (Approval Date for ANSI: July 28, 2017), IBR approved for § 170.205(b).

* * * * *

(n) * * *

(5) ONC United States Core Data for Interoperability (USCDI), Version 1 (v1), February 11, 2019, IBR approved for § 170.213; available at *https://www.healthit.gov/USCDI.*

(6) API Resource Collection in Health (ARCH) Version 1, February 1, 2019, IBR approved for § 170.215(a); available at *https://www.healthit.gov/ARCH.*

* * * * *

(p) OpenID Foundation, 2400 Camino Ramon, Suite 375, San Ramon, CA 94583, Telephone +1 925–275–6639, *http://openid.net/.*

(1) OpenID Connect Core 1.0 Incorporating Errata Set 1, November 8, 2014, IBR approved for § 170.215(b).

(2) [Reserved]

* * * * *

§ 170.300 [Amended]

■ 14. Amend § 170.300 in paragraphs (a) and (c) by removing the phrase ‘‘Complete EHRs and’’.

§ 170.314 [Removed and Reserved]

■ 15. Remove and reserve § 170.314.

■ 16. Amend § 170.315 as follows:

■ a. Remove and reserve paragraphs (a)(6) through (8), (10); (11); and (13);

■ b. In paragraphs (b)(1)(ii)(A) introductory text, (b)(1)(ii)(A)(2), (3), (b)(1)(ii)(B) and (C), remove the reference ‘‘§ 170.205(a)(3) and § 170.205(a)(4)’’ and add in its place the reference ‘‘§ 170.205(a)(3), (a)(4), and (a)(4)(i)’’;

■ c. In paragraph (b)(1)(iii) introductory text, remove the reference ‘‘§ 170.205(a)(4)’’ and add in its place the reference ‘‘§ 170.205(a)(3), (a)(4), and (a)(4)(i)’’;

■ d. Revise paragraph (b)(1)(iii)(A);

■ e. In paragraph (b)(2)(i) and (ii), remove the reference ‘‘§ 170.205(a)(3) and § 170.205(a)(4)’’ and add in its place the reference ‘‘§ 170.205(a)(3), (a)(4), and (a)(4)(i)’’;

■ f. Remove and reserve paragraphs (b)(4) through (8);

■ g. Revise paragraph (b)(9);

■ h. Add paragraphs (b)(10), (11), (12), (13),

■ i. Revise paragraph (c)(3);

■ j. Add paragraphs (d)(12), and (13);

■ k. Revise paragraph (e)(1)(i)(A)(1);

■ l. In paragraph (e)(1)(i)(B)(1)(ii) and (e)(1)(i)(B)(2) introductory text, remove the reference ‘‘§ 170.205(a)(4)’’ and add in its place the reference ‘‘§ 170.205(a)(4) and (a)(4)(i)’’;

■ m. Remove and reserve paragraph (e)(1)(ii)(B);

■ n. Remove and reserve paragraph (e)(2);

■ o. Revise paragraphs (f)(5)(iii)(B)(1), (g)(6) introductory text, (g)(6)(i) and (iv);

■ p. Revise paragraphs (g)(1) and (g)(2) by removing ‘‘EHR Incentive Programs’’ and adding in its place ‘‘Promoting Interoperability Programs’’;

■ q. Revising paragraph (g)(3)(i);

■ r. In paragraphs (g)(6)(ii) and (iii), Remove the reference ‘‘§ 170.205(a)(4)’’ and add in its place the reference ‘‘§ 170.205(a)(4) and (a)(4)(i)’’;

■ s. Revise paragraph (g)(6)(iv);

■ t. Remove paragraphs (g)(7)(ii)(A)(*3*);

■ u. Revise paragraph (g)(9)(i)(A);

■ v. Remove paragraph (g)(9)(ii)(A)(*3*); and

■ w. Add paragraphs (g)(10) and (g)(11).

The revisions and additions read as follows:

§ 170.315 2015 Edition health IT certification criteria.

* * * * *

(b) * * *

(1) * * *

(iii) * * *

(A) The data classes expressed in the standard in § 170.213 and, including as specified for the following data:

(1) Assessment and plan of treatment. In accordance with the ‘‘Assessment and Plan Section (V2)’’ of the standard specified in § 170.205(a)(4) and (a)(4)(i); or in accordance with the ‘‘Assessment Section (V2)’’ and ‘‘Plan of Treatment Section (V2)’’ of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(2) Goals. In accordance with the ‘‘Goals Section’’ of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(3) Health concerns. In accordance with the ‘‘Health Concerns Section’’ of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(4) Unique device identifier(s) for a patient’s implantable device(s). In accordance with the ‘‘Product Instance’’ in the ‘‘Procedure Activity Procedure Section’’ of the standard specified in § 170.205(a)(4) and (a)(4)(i).

* * * * *

(4) [Reserved]

(5) [Reserved]

(6) [Reserved]

(7) [Reserved]

(8) [Reserved]

(9) *Care plan.* Enable a user to record, change, access, create, and receive care plan information in accordance with:

(i) The Care Plan document template, including the Health Status Evaluations and Outcomes Section and Interventions Section (V2), in the standard specified in § 170.205(a)(4); and

(ii) The standard in § 170.205(a)(4)(i).

(10) *Electronic health information export.* (i) *Single patient electronic health information export.*

(A) Enable a user to timely create an export file(s) with all of a single patient’s electronic health information the health IT produces and electronically manages on that patient.

(B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(C) Limit the ability of users who can create such export file(s) in at least one of these two ways:

(1) To a specific set of identified users.

(2) As a system administrative function.

(D) The export file(s) created must be electronic and in a computable format.

(E) The export file(s) format, including its structure and syntax, must be included with the exported file(s).

(ii) *Database export.* Create an export of all the electronic health information the health IT produces and electronically manages.

(A) The export created must be electronic and in a computable format.

(B) The export’s format, including its structure and syntax must be included with the export.

(iii) *Documentation.* The export format(s) used to support single patient electronic health information export as specified in paragraph (b)(10)(i) of this section and database export as specified in paragraph (b)(10)(ii) of this section must be made available via a publicly accessible hyperlink.

(11) *Electronic prescribing.* (i) Enable a user to perform all of the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(1) and, at a minimum, the version of the standard specified in § 170.207(d)(3) as follows:

(A) Ask mailbox (GetMessage).

(B) Relay acceptance of transaction (Status).

(C) Error response (Error).

(D) Create new prescriptions (NewRx, NewRxRequest, NewRxResponseDenied).

(E) Change prescriptions (RxChangeRequest, RxChangeResponse).

(F) Renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(G) Resupply (Resupply).

(H) Return receipt (Verify).

(I) Cancel prescriptions (CancelRx, CancelRxResponse).

(J) Receive fill status notifications (RxFill, RxFillIndicatorChange).

(K) Drug administration (DrugAdministration).

(L) Transfer (RxTransferRequest, RxTransferResponse, RxTransferConfirm).

(M) Recertify (Recertification).

(N) Request and receive medication history (RxHistoryRequest, RxHistoryResponse).

(O) Complete risk evaluation and mitigation strategy transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(ii) For each transaction listed in paragraph (b)(11)(i) of this section, the technology must be able to receive and transmit the reason for the prescription using the diagnosis elements in DRU Segment.

(iii) *Optional.* For each transaction listed in paragraph (b)(11)(i) of this section, the technology must be able to receive and transmit the reason for the prescription using the indication elements in the SIG Segment.

(iv) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.,* not cc).

(v) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(12) *Data segmentation for privacy—send.* Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

(13) *Data segmentation for privacy—receive.* Enable a user to:

(i) Receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1); and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

(c) * * *

(3) *Clinical quality measures—report.* Enable a user to electronically create a data file for transmission of clinical quality measurement data in accordance with the implementation specifications specified in § 170.205(h)(3) and (k)(3).

* * * * *

(d) * * *

* * * * *

(12) *Encrypt authentication credentials.* Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations:

(i) ''Yes.'' Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) ''No.'' Health IT Module does not encrypt stored authentication credentials.

(13) *Multi-factor Authentication.* Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations:

(i) ''Yes.'' Health IT Module supports authentication through multiple elements the identity of the user with industry recognized standards.

(ii) ''No.'' Health IT Module does not support authentication through multiple elements the identity of the user with industry recognized standards.

(e) * * *

(1) * * *

(i) * * *

(A) * * *

(1) The data classes expressed in the standard in § 170.213 (which should be in their English (*i.e.,* non-coded) representation if they associate with a vocabulary/code set), including as specified for the following data:

(i) Assessment and plan of treatment. In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4) and (a)(4)(i); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(ii) Goals. In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(iii) Health concerns. In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(iv) Unique device identifier(s) for a patient's implantable device(s). In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

* * * * *

(ii) * * *

(B) [Reserved]

* * * * *

(f) * * *

(5) * * *

(iii) * * *

(B) * * *

(1) The data classes expressed in the standard in § 170.213.

* * * * *

(g) *Design and performance*—(1) *Automated numerator recording.* For each Promoting Interoperability Programs percentage-based measure, technology must be able to create a report or file that enables a user to review the patients or actions that would make the patient or action eligible to be included in the measure's numerator. The information in the report or file created must be of sufficient detail such that it enables a user to match those patients or actions to meet the measure's denominator limitations when necessary to generate an accurate percentage.

(2) *Automated measure Calculation.* For each Promoting Interoperability Programs percentage-based measure that is supported by a capability included in a technology, record the numerator and denominator and create a report including the numerator, denominator, and resulting percentage associated with each applicable measure.

(3) * * *

(i) User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: Paragraphs (a)(1) through (5), (9), and (14); and (b)(2), (3), and (11).

* * * * *

(6) *Consolidated CDA creation performance.* The following technical and performance outcomes must be demonstrated related to Consolidated CDA creation. The capabilities required under paragraphs (g)(6)(i) through (iv) of

this section can be demonstrated in tandem and do not need to be individually addressed in isolation or sequentially. This certification criterion's scope includes only the data classes expressed in the standard in § 170.213.

(i) *Reference C–CDA match.* Create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that matches a gold-standard, reference data file, including as specified for the following data:

(A) Assessment and plan of treatment. In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4) and (a)(4)(i); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(B) Goals. In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(C) Health concerns. In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(D) Unique device identifier(s) for a patient's implantable device(s). In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

* * * * *

(iv) *Completeness verification.* Create a data file for each of the applicable document templates referenced in paragraph (g)(6)(ii) of this section without the omission of any of the data classes expressed in the standard in § 170.213.

* * * * *

(8) [Reserved]

(9) * * *

(i) * * *

(A) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standard in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard specified in § 170.205(a)(4) and (a)(4)(i) following the CCD document template, including as specified for the following data:

(*1*) Assessment and plan of treatment. In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4) and (a)(4)(i); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(*2*) Goals. In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(*3*) Health concerns. In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(*4*) Unique device identifier(s) for a patient's implantable device(s). In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4) and (a)(4)(i).

(10) *Standardized API for patient and population services.* The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) *Data response.* Respond to requests for data (based on an ID or other token) for each of the resources referenced by the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a)(2) and (3).

(ii) *Search support.* Respond to search requests for data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) *App registration.* Enable an application to register with the technology's ''authorization server.''

(iv) *Secure connection.* Establish a secure and trusted connection with an application that requests data in accordance with the standard adopted in § 170.215(a)(5).

(v) *Authentication and app authorization—1st time connection.* The first time an application connects to request data the technology:

(A) *Authentication.* Demonstrates that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the standard adopted in § 170.215(b).

(B) *App authorization.* Demonstrates that a user can authorize applications to access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) and issue a refresh token that is valid for a period of at least 3 months.

(vi) *Authentication and app authorization—Subsequent connections.* Demonstrates that an application can access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months.

(vii) *Documentation.* (A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(*3*) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

(B) The documentation used to meet paragraph (g)(10)(vii)(A) of this section must be available via a publicly accessible hyperlink.

(11) *Consent management for APIs.* (i) Respond to requests for data in accordance with:

(A) The standard adopted in § 170.215(c)(1); and

(B) The implementation specification adopted in § 170.215(c)(2).

(ii) *Documentation.* (A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(*3*) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

(B) The documentation used to meet paragraph (g)(11)(ii)(A) of this section must be available via a publicly accessible hyperlink.

* * * * *

■ 17. Add subpart D to part 170 to read as follows:

Subpart D—Conditions and Maintenance of Certification for Health IT Developers

Subpart D—Conditions and Maintenance of Certification for Health IT Developers

§ 170.400 Basis and scope.

This subpart implements section 3001(c)(5)(D) of the Public Health Service Act by setting forth certain Conditions and Maintenance of Certification requirements for health IT developers participating in the ONC Health IT Certification Program.

§ 170.401 Information blocking.

(a) *Condition of Certification.* A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103.

(b) *Maintenance of Certification.* [Reserved]

§ 170.402 Assurances.

(a) *Condition of Certification.* (1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.

(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.

(3) A health IT developer must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification.

(4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10).

(b) *Maintenance of Certification.* (1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:

(i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or

(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.

(2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within 24 months of this final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer.

§ 170.403 Communications.

(a) *Condition of Certification.* (1) A health IT developer may not prohibit or restrict the communication regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology.

(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.

(i) *Unqualified protection for certain communications.* A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—

(A) Making a disclosure required by law;

(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;

(C) Communicating information about cybersecurity threats and incidents to government agencies;

(D) Communicating information about information blocking and other unlawful practices to government agencies; or

(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC–ACB.

(ii) *Permitted prohibitions and restrictions.* For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.

(A) *Developer employees and contractors.* A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

(B) *Non-user-facing aspects of health IT.* A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

(C) *Intellectual property.* A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's health IT (including third-party rights), provided that—

(*1*) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and

(*2*) A health IT developer does not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section.

(D) *Screenshots.* A health IT developer may require persons who communicate screenshots to—

(*1*) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(*3*) or to conceal protected health information;

(*2*) Not infringe the intellectual property rights of any third parties, provided that—

(*i*) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;

(*ii*) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work;

(*iii*) The developer has put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and

(iv) Communicators are permitted to communicate screenshots that have been redacted to not disclose third-party content; and

(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.

(E) *Pre-market testing and development.* A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.

(b) *Maintenance of Certification.* (1) *Notice.* Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:

(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(2) *Contracts and agreements.* (i) A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.

§ 170.404 Application programming interfaces.

The following Condition of Certification applies to developers of Health IT Modules certified to any of the certification criteria adopted in § 170.315(g)(7) through (11).

(a) *Condition of Certification.* (1) *General.* An API Technology Supplier must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) *Transparency conditions.* (i) *General.* The business and technical documentation published by an API Technology Supplier must be complete. All documentation published pursuant to paragraph (a)(2)(ii) of this section must be published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(ii) *Terms and conditions.* (A) *Material information.* The API Technology Supplier must publish all terms and conditions for its API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

(1) Develop software applications to interact with the API technology;

(2) Distribute, deploy, and enable the use of software applications in production environments that use the API technology;

(3) Use software applications, including to access, exchange, and use electronic health information by means of the API technology;

(4) Use any electronic health information obtained by means of the API technology; and

(5) Register software applications.

(B) *API fees.* Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(1) The persons or classes of persons to whom the fee applies;

(2) The circumstances in which the fee applies; and

(3) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

(C) *Application developer verification.* An API Technology Supplier is permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology.

(3) *Permitted fees conditions.* (i) *General conditions.* (A) All fees related to API technology not otherwise permitted by this section are prohibited from being imposed by an API Technology Supplier.

(B) For all permitted fees, an API Technology Supplier must:

(1) Ensure that fees are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(2) Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting API technology to, or at the request of, the API Data Provider to whom the fee is charged.

(3) Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers to whom the API technology is supplied, or for whom the API technology is supported.

(4) Ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

(ii) *Permitted fee—Development, deployment, and upgrades.* An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.

(iii) *Permitted fee—Supporting API uses for purposes other than patient access.* An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider. This permitted fee does not include:

(A) Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information;

(B) Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or

(C) Opportunity costs, except for the reasonable forward-looking cost of capital.

(iv) *Permitted fee—Value-added services.* An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

(v) *Record-keeping requirements.* An API Technology Supplier must keep for inspection detailed records of any fees charged with respect to the API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(4) *Openness and pro-competitive conditions. General condition.* An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

(i) *Non-discrimination.* (A) An API Technology Suppler must provide API technology to API Data Providers on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

(B) The terms on which an API Technology Supplier provides API technology must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(C) An API Technology Supplier must not offer different terms or service on the basis of:

(*1*) Whether the API User with whom an API Data Provider has a relationship is a competitor, potential competitor, or will be using electronic health information obtained via the API technology in a way that facilitates competition with the API Technology Supplier.

(*2*) The revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.

(ii) *Rights to access and use API technology.* (A) An API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment, including:

(*1*) For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier's health information technology or with health information technology under the API Technology Supplier's control;

(*2*) Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and

(*3*) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(B) An API Technology Supplier must not condition any of the rights described in paragraph (a)(4)(ii)(A) of this section on the requirement that the recipient of the rights do, or agree to do, any of the following:

(*1*) Pay a fee to license such rights, including but not limited to a license fee, royalty, or revenue-sharing arrangement.

(*2*) Not compete with the API Technology Supplier in any product, service, or market.

(*3*) Deal exclusively with the API Technology Supplier in any product, service, or market.

(*4*) Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.

(*5*) License, grant, assign, or transfer any intellectual property to the API Technology Supplier.

(*6*) Meet additional developer or product certification requirements.

(*7*) Provide the API Technology Supplier or its technology with reciprocal access to application data.

(iii) *Service and support obligations.* An API Technology Supplier must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments.

(A) *Changes and updates to API technology.* An API Technology Supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.

(B) *Changes to terms and conditions.* Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

(b) *Maintenance of Certification.* (1) *Registration for production use.* An API Technology Supplier with health IT certified to the certification criterion adopted in § 170.315(g)(10) must register and enable all applications for production use within 1 business day of completing its verification of an application developer's authenticity, pursuant to paragraph (a)(2)(ii)(C) of this section.

(2) *Service Base URL publication.* API Technology Supplier must support the publication of Service Base URLs for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider, and make such information publicly available (in a computable format) at no charge.

(3) *Rollout of (g)(10)-Certified APIs.* An API Technology Supplier with API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Data Providers with such API technology deployed with API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of this final rule's effective date.

§ 170.405 Real world testing.

(a) *Condition of Certification.* A health IT developer with Health IT Modules to be certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (11), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C. 300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b) *Maintenance of Certification.* (1) *Real world testing plan submission.* A health IT developer must submit an annual real world testing plan to its ONC–ACB via a publicly accessible hyperlink no later than December 15 of each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section.

(i) The plan must be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information.

(ii) The plan must include all health IT certified to the 2015 Edition through August 31st of the preceding year.

(iii) The plan must address the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

(A) The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability and conformance to the certification criteria's requirements, including scenario- and use case-focused testing;

(B) The care setting(s) that will be tested for real world interoperability and an explanation for the health IT developer's choice of care setting(s) to test;

(C) The timeline and plans for any voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

(D) A schedule of key real world testing milestones;

(E) A description of the expected outcomes of real world testing;

(F) At least one measurement/metric associated with the real world testing; and

(G) A justification for the health IT developer's real world testing approach.

(2) *Real world testing results reporting.* A health IT developer must submit real world testing results to its ONC–ACB via a publicly accessible hyperlink no later than January 31 each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section. The real world testing results must report the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

(i) The method(s) that was used to demonstrate real world interoperability;

(ii) The care setting(s) that was tested for real world interoperability;

(iii) The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

(iv) A list of the key milestones met during real world testing;

(v) The outcomes of real world testing including a description of any challenges encountered during real world testing; and

(vi) At least one measurement/metric associated with the real world testing.

(3) *USCDI Updates for C–CDA.* A health IT developer with health IT certified to § 170.315(b)(1), (e)(1), (g)(6), (f)(5), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(3)(i) of this section within 24 months of the effective date of this final rule.

(4) *C–CDA Companion Guide Updates.* A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (b)(9), (e)(1), (g)(6), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(4)(i) of this section within 24 months of the effective date of this final rule.

(5) *Voluntary standards and implementation specifications updates.* A health IT developer subject to paragraph (a) of this section that voluntary updates its certified health IT to a new version of an adopted standard that is approved by the National Coordinator through the Standards Version Advancement Process must:

(i) Provide advance notice to all affected customers and its ONC–ACB—

(A) Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator;

(B) The developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world;

(C) Whether the developer intends to continue to support the certificate for the existing certified Health IT Module version for some period of time and how long or if the existing certified Health IT Module version will be deprecated; and

(ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in applicable 2015 Edition certification criterion specified in paragraph (a) of this section.

§ 170.406 Attestations.

(a) *Condition of Certification.* A health IT developer must provide the Secretary with an attestation of compliance with the Conditions and Maintenance of Certification requirements specified in §§ 170.401 through 170.405 at the time of certification. Specifically, a health IT developer must attest to:

(1) Having not taken any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103;

(2) Having provided assurances satisfactory to the Secretary that they will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information;

(3) Not prohibiting or restricting the communications regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology; and

(4) Having published application programming interfaces (APIs) and allowing health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws;

(5) Ensuring that its health IT allows for health information to be exchanged, accessed, and used, in the manner described in paragraph (a)(4) of this section; and

(6) Having undertaken real world testing of its Health IT Module(s) for interoperability (as defined in 42 U.S.C. 300jj(9)) in the type of setting in which such Health IT Module(s) will be/is marketed.

(b) *Maintenance of Certification.* (1) A health IT developer must attest to compliance with §§ 170.401 through 170.405 at the time of certification.

(2) A health IT developer must attest semiannually to compliance with §§ 170.401 through 170.405 for all its health IT that had an active certification at any time under the ONC Health IT Certification Program during the prior six months.

§ 170.501 [Amended]

■ 18. Amend § 170.501 as follows:

■ a. In paragraph (a) remove the phrase ‘‘Complete EHRs’’;

■ b. In paragraph (b) remove the phrase ‘‘Complete EHRs and’’; and

■ c. Remove and reserve paragraph (c).

§ 170.502 [Amended]

■ 19. Amend § 170.502 as follows:

■ a. In the definition of ‘‘Deployment site’’, remove the phrase ‘‘Complete EHR,’’;

■ b. In the definition of ‘‘Development site’’, remove the phrase ‘‘Complete EHR,’’;

■ c. In the definition of ‘‘Gap certification’’, remove the phrase ‘‘Complete EHR or’’;

■ d. Remove the definition of ‘‘ONC-Approved Accreditor or ONC–AA’’;

■ e. In the definition of ‘‘ONC-Authorized Certification Body or ONC–ACB’’, remove the phrase ‘‘Complete EHRs,’’; and

■ f. In the definition of ‘‘ONC-Authorized Testing Lab or ONC–ATL’’, remove the phrase ‘‘Complete EHRs and’’.

§ 170.503 [Removed and Reserved]

■ 20. Remove and reserve § 170.503.

§ 170.504 [Removed and Reserved]

■ 21. Remove and reserve § 170.504.

■ 22. Revise § 170.505 to read as follows:

§ 170.505 Correspondence.

(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC–ACB status, an applicant for ONC–ATL status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.

(b) In circumstances where it is necessary for an applicant for ONC–ACB status, an applicant for ONC–ATL status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the official date of receipt for all parties will be the date of the delivery confirmation to the address on record.

§ 170.510 [Amended]

■ 23. Amend § 170.510 by removing paragraph (a) and redesignating paragraphs (b) and (c) as paragraphs (a) and (b).

■ 24. Amend § 170.520 by revising paragraph (a)(3) to read as follows:

§ 170.520 Application.

(a) * * *

(3) Documentation that confirms that the applicant has been accredited to ISO/IEC 17065, with an appropriate scope, by any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF) (incorporated by reference in § 170.599).

* * * * *

■ 25. Amend § 170.523 as follows:

■ a. Revise paragraph (a);

■ b. In paragraph (f) introductory text, add a header and remove the phrase, ‘‘Complete EHRs,’’;

■ c. Removing and reserve paragraph (f)(2);

■ d. Revise paragraphs (g) and (h);

■ e. In paragraph (k) introductory text, remove the phrase ‘‘Complete EHRs and’’;

■ f. In paragraph (k)(1) introductory text, add a header and remove the phrase ‘‘Complete EHR or’’;

■ g. Remove paragraphs (k)(1)(ii)(B), and (k)(1)(iii)(B);

■ h. Revise paragraph (k)(1)(iii)(A);

■ i. Remove paragraphs (k)(1)(iv)(B) and (C);

■ j. Remove and reserve paragraphs (k)(2) and (3);

■ k. Revise paragraph (k)(4);

■ l. Revise paragraphs (m)(1) and (2);

■ m. Add paragraphs (m)(3) and (4));

■ n. In paragraph (o), remove the phrase ‘‘Complete EHR or’’; and

■ o. Add paragraphs (p) through (t).

The revisions and additions read as follows:

§ 170.523 Principles of proper conduct for ONC–ACBs.

* * * * *

(a) *Accreditation.* Maintain its accreditation in good standing to ISO/IEC 17065 (incorporated by reference in § 170.599).

* * * * *

(f) *Reporting.* * * *

(2) [Reserved]

(g) *Records retention.* (1) Retain all records related to the certification of Complete EHRs and Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (g)(1) of this section;

(h) *Testing.* Only certify Health IT Modules that have been:

(1) Tested, using test tools and test procedures approved by the National Coordinator, by an:

(i) ONC–ATL;

(ii) ONC–ATL, NVLAP-accredited testing laboratory under the ONC Health IT Certification Program, and/or an ONC–ATCB for the purposes of performing gap certification; or

(2) Evaluated by it for compliance with a conformance method approved by the National Coordinator.

* * * * *

(k) *Disclosures.* * * *

(1) * * *

(ii) For a Health IT Module certified to 2015 Edition health IT certification criteria, the information specified by paragraphs (f)(1)(i), (vi) through (viii), (xv), and (xvi) of this section as applicable for the specific Health IT Module.

(iii) In plain language, a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module’s capabilities, whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT’s certification. The additional types of costs or fees required to be disclosed include but are not limited to costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

* * * * *

(2) [Reserved]

(3) [Reserved]

(4) A certification issued to a Health IT Module based solely on the applicable certification criteria adopted by the ONC Health IT Certification Program must be separate and distinct from any other certification(s) based on other criteria or requirements.

* * * * *

(m) * * *

(1) All adaptations of certified Health IT Modules;

(2) All updates made to certified Health IT Modules affecting the capabilities in certification criteria to which the ‘‘safety-enhanced design’’ criteria apply;

(3) All updates made to certified Health IT Modules in compliance with § 170.405(b)(3) and (4); and;

(4) All voluntary standards updates successfully made to certified Health IT Modules per § 170.405(b)(5).

* * * * *

(p) *Real world testing.* (1) Review and confirm that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1).

(2) Review and confirm that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2).

(3) Submit real world testing plans by December 15 of each calendar year and results by April 1 of each calendar year to ONC for public availability.

(q) *Attestations.* Review and submit health IT developer Conditions and Maintenance of Certification attestations made in accordance with § 170.406 to ONC for public availability.

(r) *Test results from ONC–ATLs.* Accept test results from any ONC–ATL that is:

(1) In good standing under the ONC Health IT Certification Program, and

(2) Compliant with its ISO 17025 accreditation requirements.

(s) *Information for direct review.* Report to ONC, no later than a week after becoming aware of, any information that could inform whether ONC should exercise direct review under § 170.580(a).

(t) *Standards Voluntary Advancement Process Module Updates Notices.* Ensure health IT developers opting to take advantage of the Standards Version Advancement Process flexibility per § 170.405(b)(5) provide timely advance written notice to the ONC–ACB and all affected customers.

(1) Maintain a record of the date of issuance and the content of developers' § 170.405(b)(5) notices; and

(2) Timely post content of each § 170.405(b)(5) notice received publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies.

■ 26. Amend § 170.524 as follows:

■ a. Revise paragraph (f); and

■ b. In paragraph (h)(3), remove the phrase ''Complete EHRs and/or''. The revisions and additions read as follows:

§ 170.524 Principles of proper conduct for ONC–ATLs.

* * * * *

(f) *Records retention.* (1) Retain all records related to the testing of Complete EHRs and/or Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (f)(1) of this section;

* * * * *

§ 170.545 [Removed and Reserved]

■ 27. Remove and reserve § 170.545.

■ 28. Amend § 170.550 as follows:

■ a. Add paragraph (e);

■ b. Remove and reserve paragraph (f);

■ c. Add paragraph (g)(5);

■ d. Revise paragraphs (h)(3)(i), (iii), (v), (vii); and

■ e. Add paragraphs (h)(3)(ix) and (l).

The additions and revisions read as follows:

§ 170.550 Health IT Module certification.

* * * * *

(e) ONC–ACBs must provide an option for certification of Health IT Modules to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification through the Standards Version Advancement Process.

(f) [Reserved]

(g) * * *

(5) Section 170.315(b)(10) when the health IT developer of the health IT presented for certification produces and electronically manages electronic health information.

(h) * * *

(3) * * *

(i) Section 170.315(a)(1) through (3), (5) through (8), (11), and (12) are also certified to the certification criteria specified in § 170.315(d)(1) through (7). Section 170.315(a)(4), (9), (10), and (13) are also certified to the certification criteria specified in § 170.315(d)(1) through (3), and (5) through (7).

* * * * *

(iii) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1), (2)(i)(A), (B), (ii) through (v), (3), and (5);

* * * * *

(v) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A), (B), (ii) through (v), (3), (5), and (9);

* * * * *

(vii) Section 170.315(g)(7) through (11) is also certified to the certification criteria specified in § 170.315(d)(1) and (9); and (d)(2)(i)(A), (2)(i)(B), 2(ii) through (v), or (10);

(viii) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1), (2)(i)(A), (2)(i)(B), (2)(ii) through (v), and (3); and

* * * * *

(ix) If applicable, any criterion adopted in § 170.315 is also certified to the certification criteria specified in § 170.315(d)(12) and/or (13).

* * * * *

(l) *Conditions of Certification Attestations.* Before issuing a certification, ensure that the health IT developer of the Health IT Module has met its responsibilities under subpart D of this part.

§ 170.555 [Amended]

■ 29. Amend § 170.555 as follows:

■ a. In paragraph (a), remove the reference ''Complete EHRs and/or'';

■ b. Revise paragraph (b)(1); and

■ c. In paragraph (b)(2), remove the reference ''certified Complete EHR or''. The revisions read as follows:

§ 170.555 Certification to newer versions of certain standards.

* * * * *

(b) * * *

(1) ONC–ACBs are not required to certify Complete EHRs and/or Health IT Module(s) according to newer versions of standards adopted and named in subpart B of this part, unless:

(i) The National Coordinator identifies a new version through the Standards Version Advancement Process and a health IT developer voluntarily elects to update its certified health IT to the new version in accordance with § 170.405(b)(5); or

(ii) The new version is incorporated by reference in § 170.299.

* * * * *

■ 30. Amend § 170.556 as follows:

■ a. Revise paragraph (a) introductory text;

■ b. In paragraph (b) introductory text, remove the phrase ''certified Complete EHR or'';

■ c. Revise paragraph (c) introductory text;

■ d. In paragraph (c)(1), remove the phrases ''certified Complete EHR or'' and ''Complete EHR or'';

■ e. Remove and reserve paragraph (c)(2);

■ f. In paragraph (c)(3), remove the phrase ''certified Complete EHRs and'';

■ g. In paragraphs (c)(4)(i) and (ii), remove the phrase ''certified Complete EHR or'';

■ h. Remove paragraphs (c)(5) and (6);

■ i. In paragraph (d)(1), remove the phrase ''Complete EHR or'';

■ j. In paragraph (d)(3)(ii), remove the phrase ''certified Complete EHR or'';

■ k. In paragraph (d)(5) introductory text, remove the phrase ''Complete EHR or'';

■ l. In paragraph (d)(6), remove the phrases ''certified Complete EHR or'' and ''Complete EHR or'';

■ m. In paragraph (e)(3), remove the phrase ''Complete EHR or''; and

■ n. In paragraph (f), remove the phrase ''certified Complete EHR or''. The revisions and additions read as follows:

§ 170.556 In-the-field surveillance and maintenance of certification for Health IT.

(a) *In-the-field surveillance.* Consistent with its accreditation to ISO/IEC 17065 and the requirements of this subpart, an ONC–ACB must initiate surveillance ''in the field'' as necessary to assess whether a certified Health IT Module continues to conform to the requirements in subparts A, B, C and E of this part once the certified Health IT Module has been implemented and is in use in a production environment.

* * * * *

(c) *Randomized surveillance.* During each calendar year surveillance period, an ONC–ACB may conduct in-the-field surveillance for certain randomly selected Health IT Modules to which it has issued a certification.

* * * * *

(2) [Reserved]

* * * * *

§§ 170.560, 170.565, and 170.570 [Amended]

■ 31. In the table below, for each section and paragraph indicated in the first two columns, remove the phrase indicated in the third column:

Section	Paragraphs	Remove
§ 170.560	(a)(2)	''Complete EHRs and/or''.
§ 170.565	(d)(ii) and (d)(iii)	''Complete EHRs or''.
§ 170.565	(h)(2)(iii)	''Complete EHRs and''.
§ 170.570	(a), (b)(2), (c) introductory text, (c)(1), and (c)(2)	''Complete EHRs and/or''.

§ 170.575 [Removed and Reserved]

■ 32. Remove and reserve § 170.575.

■ 33. Amend § 170.580 as follows:

■ a. Revise paragraph (a)(1) and the headings of paragraphs (a)(2)(i) and (ii);

■ b. Add paragraph (a)(2)(iii);

■ c. Revise paragraphs (a)(3)(i), (iv), and (v);

■ d. Add paragraph (a)(4);

■ e. Revise paragraphs (b)(1)(i) and (iii)(D);

■ f. Revise paragraphs (b)(2)(i);

■ g. Revise paragraphs (b)(3)(i) and (ii);

■ h. Add paragraphs (b)(3)(iii) and (iv);

■ i. Revise paragraph (c)(1);

■ j. In paragraphs (d)(1), (d)(2)(i)(C), and (d)(4), remove the phrase ''Complete EHR or'';

■ k. In paragraph (d)(5), remove the phrase ''Complete EHRs or'';

■ l. Revise paragraph (e)(1) introductory text;

■ m. Revise paragraph (f)(1);

■ n. In paragraph (f)(2)(i)(C) by removing the reference ''Complete EHR or'';

■ o. Revise paragraphs (g)(1) introductory text, (g)(1)(i), (g)(2), (g)(3)(i), (g)(4), (g)(5)(i), and (g)(6)(v).

The additions and revisions read as follows:

§ 170.580 ONC review of certified health IT or a health IT developer's actions.

(a) * * *

(1) *Purpose.* ONC may directly review certified health IT or a health IT developer's actions or practices to determine whether either conform to the requirements of the ONC Health IT Certification Program.

(2) * * *

(i) *Certified health IT causing or contributing to unsafe conditions.* * * *

* * * * *

(ii) *Impediments to ONC–ACB oversight of certified health IT.* * * *

* * * * *

(iii) *Noncompliance with Conditions and Maintenance of Certification.* ONC may initiate direct review under this section if it has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement under subpart D of this part.

(3) * * *

(i) ONC's review of certified health IT or a health IT developer's actions or practices is independent of, and may be in addition to, any surveillance of certified health IT conducted by an ONC–ACB.

(4) *Coordination with the Office of Inspector General.* (i) ONC may coordinate its review of a claim of information blocking with the Office of Inspector General or defer to the Office of Inspector General to lead a review of a claim of information blocking.

(ii) ONC may rely on Office of Inspector General findings to form the basis of a direct review action.

* * * * *

(iv) An ONC–ACB and ONC–ATL shall provide ONC with any available information that ONC deems relevant to its review of certified health IT or a health IT developer's actions or practices.

(v) ONC may end all or any part of its review of certified health IT or a health IT developer's actions or practices under this section at any time and refer the applicable part of the review to the relevant ONC–ACB(s) if ONC determines that doing so would serve the effective administration or oversight of the ONC Health IT Certification Program.

(b) * * *

(1) * * *

(i) *Circumstances that may trigger notice of potential non-conformity.* At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of potential non-conformity if it has a reasonable belief that certified health IT or a health IT developer may not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(iii) * * *

(D) Issue a notice of proposed termination if the health IT is under review in accordance with paragraphs (a)(2)(i) or (ii) of this section.

(2) * * *

(i) *Circumstances that may trigger notice non-conformity.* At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of non-conformity to the health IT developer if it determines that certified health IT or a health IT developer's actions or practices does not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(*3*) * * *

(i) All records related to the development, testing, certification, implementation, maintenance and use of its certified health IT;

(ii) Any complaint records related to the certified health IT;

(iii) All records related to the Condition(s) and Maintenance of Certification requirements, including marketing and distribution records, communications, and contracts; and

(iv) Any other relevant information.

(c) * * *

(1) *Applicability.* If ONC determines that certified health IT or a health IT developer's action or practice does not conform to requirements of the ONC Health IT Certification Program, ONC shall notify the health IT developer of its determination and require the health

IT developer to submit a proposed corrective action plan.

* * * * *

(e) * * *

(1) *Applicability.* Excluding situations of noncompliance with a Condition or Maintenance of Certification requirement under subpart D of this part, ONC may propose to terminate a certification issued to a Health IT Module if:

* * * * *

(f) * * *

(1) *Applicability.* The National Coordinator may terminate a certification if:

(i) A determination is made that termination is appropriate after considering the information provided by the health IT developer in response to the proposed termination notice;

(ii) The health IT developer does not respond in writing to a proposed termination notice within the timeframe specified in paragraph (e)(3) of this section; or

(iii) A determination is made that the health IT developer is noncompliant with a Condition or Maintenance of Certification requirement under subpart D of this part or for the following circumstances when ONC exercises direct review under paragraph (a)(2)(iii) of this section:

(A) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

(*1*) Fact-finding;

(*2*) A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(*3*) of this section; or

(*3*) A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(*3*) of this section.

(B) The information or access provided by the health IT developer in response to any ONC communication, including, but not limited to: Fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete;

(C) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(D) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(E) The health IT developer fails to timely submit a corrective action plan that adequately addresses the elements required by ONC as described in paragraph (c) of this section;

(F) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(G) ONC concludes that the non-conformity(ies) cannot be cured.

* * * * *

(g) * * *

(1) *Basis for appeal.* A health IT developer may appeal an ONC determination to suspend or terminate a certification issued to a Health IT Module and/or an ONC determination to issue a certification ban under § 170.581(a)(2) if the health IT developer asserts:

(i) ONC incorrectly applied ONC Health IT Certification Program requirements for a

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2); or

* * * * *

(2) *Method and place for filing an appeal.* A statement of intent to appeal followed by a request for appeal must be submitted to ONC in writing by an authorized representative of the health IT developer subject to the determination being appealed. The statement of intent to appeal and request for appeal must be filed in accordance with the requirements specified in the notice of:

(i) Termination;

(ii) Suspension; or

(iii) Certification ban under § 170.581(a)(2).

(3) * * *

(i) A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

* * * * *

(4) *Effect of appeal.* (i) A request for appeal stays the termination of a certification issued to a Health IT Module, but the Health IT Module is prohibited from being marketed, licensed, or sold as ''certified'' during the stay.

(ii) A request for appeal does not stay the suspension of a Health IT Module.

(iii) A request for appeal stays a certification ban issued under § 170.581(a)(2).

(5) * * *

(i) The hearing officer may not review an appeal in which he or she participated in the initial suspension, termination, or certification ban determination or has a conflict of interest in the pending matter.

* * * * *

(6) * * *

(v) ONC will have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf that clarifies, as necessary, its determination to suspend or terminate the certification or issue a certification ban.

* * * * *

■ 34. Revise § 170.581 to read as follows:

§ 170.581 Certification ban.

(a) *Circumstances trigger a certification ban.* The certification of any of a health IT developer's health IT is prohibited when:

(1) The certification of one or more of the health IT developer's Complete EHRs or Health IT Modules is:

(i) Terminated by ONC under the ONC Health IT Certification Program;

(ii) Withdrawn from the ONC Health IT Certification Program by an ONC–ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(iii) Withdrawn by an ONC–ACB because of a non-conformity with any of the certification criteria adopted by the Secretary under subpart C of this part;

(iv) Withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary under subpart C of this part, including notice of pending surveillance; or

(2) ONC determines a certification ban is appropriate per its review under § 170.580(a)(2)(iii).

(b) *Notice of certification ban.* When ONC decides to issue a certification ban to a health IT developer, ONC will notify the health IT developer of the certification ban through a notice of certification ban. The notice of certification ban will include, but may not be limited to:

(1) An explanation of the certification ban;

(2) Information supporting the certification ban;

(3) Instructions for appealing the certification ban if banned in accordance with paragraph (a)(2) of this section; and

(4) Instructions for requesting reinstatement into the ONC Health IT Certification Program, which would lift the certification ban.

(c) *Effective date of certification ban.* (1) A certification ban will be effective immediately if banned under paragraphs (a)(1) of this section.

(2) For certification bans issued under paragraph (a)(2) of this section, the ban

will be effective immediately after the following applicable occurrence:

(i) The expiration of the 10-day period for filing a statement of intent to appeal in § 170.580(g)(3)(i) if the health IT developer does not file a statement of intent to appeal.

(ii) The expiration of the 30-day period for filing an appeal in § 170.580(g)(3)(ii) if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(iii) A final determination to issue a certification ban per § 170.580(g)(7) if a health IT developer files an appeal timely.

(d) *Reinstatement.* The certification of a health IT developer's health IT subject to the prohibition in paragraph (a) of this section may commence once the following conditions are met.

(1) A health IT developer must request ONC's permission in writing to participate in the ONC Health IT Certification Program.

(2) The request must demonstrate that the customers affected by the certificate termination, certificate withdrawal, or non-compliance with a Condition or Maintenance of Certification have been provided appropriate remediation.

(3) For non-compliance with a Condition or Maintenance of Certification requirement, the non-compliance must be resolved.

(4) ONC is satisfied with the health IT developer's demonstration under paragraph (d)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

■ 35. Add part 171 to read as follows:

PART 171—INFORMATION BLOCKING

Subpart A—General Provisions

Subpart B—Exceptions for Reasonable and Necessary Activities That Do Not Constitute Information Blocking

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

Subpart A—General Provisions

§ 171.100 Statutory basis and purpose.

(a) *Basis.* This part implements section 3022 of the Public Health Service Act, 42 U.S.C. 300jj–52.

(b) *Purpose.* The purpose of this part is to establish exceptions for reasonable and necessary activities that do not constitute ''information blocking,'' as defined by section 3022(a)(1) of the Public Health Service Act, 42 U.S.C. 300jj–52.

§ 171.101 Applicability.

This part applies to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks, as those terms are defined in § 171.102.

§ 171.102 Definitions.

For purposes of this part:

Access means the ability or means necessary to make electronic health information available for use, including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained.

Actor means a health care provider, health IT developer of certified health IT, health information exchange, or health information network.

API Data Provider is defined as it is in § 170.102.

API Technology Supplier is defined as it is in § 170.102.

Electronic Health Information (EHI) means—

(1) Electronic protected health information; and

(2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Electronic media is defined as it is in 45 CFR 160.103.

Electronic protected health information (ePHI) is defined as it is in 45 CFR 160.103.

Exchange means the ability for electronic health information to be transmitted securely and efficiently between and among different technologies, systems, platforms, or networks in a manner that allows the information to be accessed and used.

Fee means any present or future obligation to pay money or provide any other thing of value.

Health care provider has the same meaning as ''health care provider'' at 42 U.S.C. 300jj.

Health Information Exchange or *HIE* means an individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes.

Health Information Network or *HIN* means an individual or entity that satisfies one or both of the following—

(1) Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

(2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

Health IT developer of certified health IT means an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program.

Information blocking is defined as it is in § 171.103 and 42 U.S.C. 300jj–52(a).

Interfere with means to prevent, materially discourage, or otherwise inhibit access, exchange, or use of electronic health information.

Interoperability element means—

(1) Any functional element of a health information technology, whether hardware or software, that could be used to access, exchange, or use electronic health information for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.

(2) Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology,

including for the purpose of developing compatible technologies that incorporate or use the functional elements.

(3) Any technology or service that may be required to enable the use of a compatible technology in production environments, including but not limited to any system resource, technical infrastructure, or health information exchange or health information network element.

(4) Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.

(5) Any other means by which electronic health information may be accessed, exchanged, or used.

Permissible purpose means a purpose for which a person is authorized, permitted, or required to access, exchange, or use electronic health information under applicable law.

Person is defined as it is in 45 CFR 160.103.

Protected health information is defined as it is in 45 CFR 160.103.

Practice means one or more related acts or omissions by an actor.

Use means the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.

§ 171.103 Information blocking.

Information blocking means a practice that—

(a) Except as required by law or covered by an exception set forth in subpart B of this part, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and

(b) If conducted by a health information technology developer, health information exchange, or health information network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or

(c) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Subpart B—Exceptions for Reasonable and Necessary Activities That Do Not Constitute Information Blocking

§ 171.200 Availability and effect of exceptions.

A practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision by meeting all applicable requirements and conditions of the exception at all relevant times.

§ 171.201 Exception—Preventing harm.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from—

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; or

(3) Disclosure of a patient's electronic health information in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be—

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; and

(4) No broader than necessary to mitigate the risk of harm.

(c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

§ 171.202 Exception—Promoting the privacy of electronic health information.

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) *Meaning of "individual" in this section.* The term "individual" as used in this section means one or more of the following—

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under State or other law.

(b) *Precondition not satisfied.* If the actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information, the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that—

(1) The actor's practice—

(i) Conforms to the actor's organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; and

(C) Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; or

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor's practice is—

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

(c) *Health IT developer of certified health IT not covered by HIPAA.* If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the actor may choose not to provide access, exchange, or use of electronic health information provided that the actor's practice—

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) *Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3).* If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) *Respecting an individual's request not to share information.* In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

§ 171.203 Exception—Promoting the security of electronic health information.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; and

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

§ 171.204 Exception—Recovering costs reasonably incurred.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Types of costs to which this exception applies.* This exception is limited to the actor's costs reasonably incurred to provide access, exchange, or use of electronic health information.

(b) *Method for recovering costs.* The method by which the actor recovers its costs—

(1) Must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests;

(2) Must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged;

(3) Must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported;

(4) Must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor; and

(5) Must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information.

(c) *Costs specifically excluded.* This exception does not apply to—

(1) Costs that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using electronic health information;

(2) Costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets;

(3) Opportunity costs, except for the reasonable forward-looking cost of capital;

(4) A fee prohibited by 45 CFR 164.524(c)(4);

(5) A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's electronic health information;

(6) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; or

(7) A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

(d) *Compliance with the Conditions of Certification.* (1) Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4) or § 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(2) If the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404 of this subchapter.

§ 171.205 Exception—Responding to requests that are infeasible.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Request is infeasible.* (1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—

(i) The type of electronic health information and the purposes for which it may be needed;

(ii) The cost to the actor of complying with the request in the manner requested;

(iii) The financial, technical, and other resources available to the actor;

(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

(vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and

(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.

(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.

(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(b) *Responding to requests.* The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.

(c) *Written explanation.* The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(d) *Provision of a reasonable alternative.* The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information.

§ 171.206 Exception—Licensing of interoperability elements on reasonable and non-discriminatory terms.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Responding to requests.* Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:

(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and

(2) Offering an appropriate license with reasonable and non-discriminatory terms.

(b) *Reasonable and non-discriminatory terms.* The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.

(1) *Scope of rights.* The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.

(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.

(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(2) *Reasonable royalty.* If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies.

(3) *Non-discriminatory terms.* The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements.

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on—

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

(4) *Collateral terms.* The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

(5) *Non-disclosure agreement.* The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided—

(i) The agreement states with particularity all information the actor claims as trade secrets; and

(ii) Such information meets the definition of a trade secret under applicable law.

(c) *Additional requirements relating to the provision of interoperability elements.* The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

(3) Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

(d) *Compliance with conditions of certification.* Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the conditions of certification in §§ 170.402, 170.403, or 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

§ 171.207 Exception—Maintaining and improving health IT performance.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) *Maintenance and improvements to health IT.* An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—

(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

(b) *Practices that prevent harm.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(c) *Security-related practices.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

Dated: January 22, 2019.

Alex M. Azar II,

Secretary, Department of Health and Human Services.

Note: The following appendix will not appear in the Code of Federal Regulations.

Appendix: Pediatric Technical Worksheets

These worksheets contain information on how each recommendation corresponds to the Children's EHR Format and to the existing or proposed new ONC certification criteria. We invite readers to use these worksheets to inform public comment on the recommendations, the inclusion of specific items from the Children's EHR Format,[193] and the identified certification criteria as they relate specifically to use cases for pediatric care and sites of service.

We welcome public comment on the identified certification criteria for each recommendation. Specifically, we seek comment for each recommendation on the following four broad questions:

- *Q1.* What relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) may impact or support feasibility of the recommendation in practice?
- *Q2.* How can the effective use of IT support each recommendation as involves provider training, establishing workflow, and other related safety and usability considerations?
- *Q3.* Should any of the recommendations *not* be included?
- *Q4.* Should any of the functional criteria listed under the ''Alignment with 2015 Edition Certification Criteria'' and the ''Alignment with Proposed New or Updated Certification Criteria'' be removed as a correlated item to support any of the recommendations?

Commenters are encouraged to reference the specific recommendation number (110) with the corresponding question number in their response. For example, ''Recommendation 1. Q3.'' Commenters are highly encouraged to use the template ONC has created to support public comment on the proposed rule.

Recommendation 1: Use Biometric-Specific Norms for Growth Curves and Support Growth Charts for Children

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Use biometric-specific norms for growth curves.

Children's EHR Format: Req-2044—Release Package 2015 Priority List.

Topic(s): Primary Care Management, Well Child/Preventive Care.

Description: The system shall include the ability to use pediatric age-specific norms for weight, height/length, head circumference, and BMI to calculate and display growth percentiles and plot them over time on standardized Centers for Disease Control and Prevention/World Health Organizations (CDC/WHO) growth curves as appropriate.

Alignment With 2015 Edition Certification Criteria

ONC believes this recommendation is supported by the 2015 Edition definition and criteria listed below:

Common Clinical Data Set (CCDS)* including *optional* pediatric vital sign data elements with the reference range/scale or growth curve for BMI percentile per age and sex for youth 2–20 years of age, weight for age per length and sex for children less than three years of age, and head occipital-frontal circumference for children less than three years of age.

Demographic criterion requires the ability to record birth sex in accordance with HL7 Version 3 (''Administrative Gender'') and a null flavor value attributed as follows: Male (M); female (F); and unknown (UNK).

Clinical Decision Support (CDS) can be used to develop a variety of tools to enhance decision-making in the pediatric clinical workflow including contextually relevant reference information, clinical guidelines, condition-specific order sets, alerts, and reminders, among other tools.

Application Programming Interfaces criteria including the ''application access—patient selection'', ''application access—data category request'', and ''application access—all data request'' which can help address many of the challenges currently faced by caregivers accessing pediatric health data.

Alignment With Proposed New or Updated Certification Criteria

ONC believes this recommendation is supported by the proposed new and updated certification criteria in this proposed rule:

United States Core Data for Interoperability (USCDI): The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.

Application Programming Interfaces (APIs): § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for

[193] *https://healthit.ahrq.gov/health-it-tools-and-resources/pediatric-resources/childrens-electronic-health-record-ehr-format.*

interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Supplemental Children's Format Requirements for Recommendation 1

We seek feedback about the relevance of the following potential supplemental Children's EHR Format requirements and their correlation to Recommendation 1.

1. *Title:* Allow unknown patient sex.

Children's EHR Format: Req-2009—Release Package 2015 Priority List.

Topic(s): Prenatal Screening, Birth Information, Genetic information.

Description: The system shall provide the ability to record a patient's sex as male, female, or unknown, and shall allow it to be updated.

2015 Edition Criterion Alignment: Demographics.

New or Updated Criterion Alignment: USCDI.

2. *Title:* Record Gestational Age Assessment and Persist in the EHR.

Children's EHR Format: Requirement Req-2019—Release Package 2015 Priority List.

Topic(s): Well Child/Preventive Care, Growth Data.

Description: The system shall capture and display assigned gestational age as well as the diagnosis of SGA (Small for Gestational Age) or LGA (Large for Gestational Age) when appropriate.

2015 Edition Criterion Alignment: Common Clinical Data Set (CCDS).

New or Updated Criterion Alignment: USCDI.

3. *Title:* Support growth charts for children.

Children's EHR Format: Requirement Req-2042—Release Package: 2015 Priority List.

Topic(s): Growth Data.

Description: The system shall support display of growth charts that plot selected growth parameters such as height, weight, head circumference, and BMI (entered with appropriate precision or computed as described in Req-2019) along with appropriate sets of norms provided by the CDC or in a compatible tabular format (typically based on Lambda-Mu-Sigma [LMS] curve fitting computational method).

2015 Edition Criterion Alignment: Common Clinical Data Set (CCDS), Clinical Decision Support (CDS).

New or Updated Criterion Alignment: USCDI, API.

Title: Provide alerts for out-of-range biometric data.

Children's EHR Format: Requirement Req-2045—Release Package 2015 Priority List.

Topic(s): Primary Care Management, Well Child/Preventive Care.

Description: The system shall include the ability to provide alerts for weight, length/height, head circumference, and BMI data points that fall outside two standard deviations of CDC/WHO pediatric data.

2015 Edition Criterion Alignment: Clinical Decision Support (CDS).

New or Updated Criterion Alignment: USCDI, API.

Recommendation 2: Compute Weight-Based Drug Dosage

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Compute weight-based drug dosage.

Children's EHR Format: Req-2012—Release Package 2015 Priority List.

Topic(s): Medication Management.

Description: The system shall compute drug dose, based on appropriate dosage ranges, using the patient's body weight and body surface area, and shall display the dosing weight and weight-based dosing strategy (when applicable) on the prescription.

Alignment With 2015 Edition Certification Criterion

ONC believes this recommendation is supported by the 2015 Edition criterion listed below:

- *Electronic Prescribing* criterion:

—Provides the ability to send and receive the specified prescription transactions electronically per the NCPDP SCRIPT Version 10.6 Standard Implementation Recommendations and using RxNorm vocabulary codes

—Limits the ability to prescribe all oral, liquid medications in only metric standard units of mL (*i.e.,* not cc)

Includes an *optional* Structured and Codified Sig Format, which has the capability to exchange weight-based dosing calculations within the NCPDP SCRIPT 10.6 standard.

Alignment With Proposed New or Updated Certification Criteria

ONC believes this recommendation is supported by the proposed new and updated certification criteria in this proposed rule:

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Electronic Prescribing:* (§ 170.315(b)(11)) which supports improved patient safety and prescription accuracy, workflow efficiencies, and increase configurability of systems including functionality that would support pediatric medication management.

Supplemental Children's Format Requirements for Recommendation 2

We seek feedback about the relevance of the following potential Children's EHR Format requirements and their correlation to Recommendation 2.

1. *Title:* Rounding for administrable doses.

Children's EHR Format: Req-2035—Release Package 2015 Priority List.

Topic(s): Medication Management.

Description: The system shall enable calculated doses (*e.g.,* weight-based) to be rounded to optimize administration convenience.

2015 Edition Criterion Alignment: Electronic prescribing.

New or Updated Criterion Alignment: Electronic prescribing.

2. *Title:* Alert based on age-specific norms.

Children's EHR Format: Req-2013—Release Package 2015 Priority List.

Topic(s): Primary Care Management, Well Child/Preventive Care.

Description: The system shall provide the ability to present alerts for lab results outside of pediatric-specific normal value ranges.

2015 Edition Criterion Alignment: Clinical decision support (CDS).

New or Updated Criterion Alignment: API.

Recommendation 3: Ability To Document All Guardians and Caregivers

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Ability to access family history, including all guardians and caregivers.

Children's EHR Format: Req-2006—Release Package 2015 Priority List.

Topic(s): Child Abuse Reporting, Primary Care Management, Parents and Guardians, and Family Relationship Data.

Description: The system shall provide the ability to record information about all guardians and caregivers (biological parents, foster parents, adoptive parents, guardians, surrogates, and custodians), siblings, and case workers, with contact information for each.

Alignment With 2015 Edition Certification Criteria

ONC believes this recommendation is supported by the 2015 Edition criteria listed below, and ONC believes this priority also is supported by health IT beyond what is included in the certification program.

- *Care Plan:* Criteria includes the ability to record, change, access, create, and receive care plan information according to the care plan document template in the HL7 implementation guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), draft standard for Trial Use Release 2.1 (including the sections for health status evaluations and outcomes and for interventions (V2)).
- *Transitions of Care:* Criteria includes the ability to create, receive, and properly consumer interoperable documents using a common content and transport standard that include key health data that should be accessible and available for exchange.
- *Application Programming Interfaces* criteria including the ''application access—patient selection'', ''application access—data category request'', and ''application access—all data request'' which can help address many of the challenges currently faced by caregivers accessing pediatric health data.
- *Transitions of Care* criteria includes the ability to create and to receive interoperable documents using a comment content standard that include key health data that should be accessible and available for exchange to support the care of children across care settings.
- *Demographic* criterion requires the ability to record various demographic information for a patient including potential supports for patient and parental matching.

Alignment With Proposed New or Updated Certification Criteria

ONC believes tis priority is supported by the proposed new and updated certification criteria in this proposed rule:

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Data Segmentation for Privacy:* (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) could provide functionality to address the concerns multiple stakeholders expressed regarding the need to restrict granular pediatric health data at production based on the intended recipient of the data.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Supplemental Children's EHR Format Requirements for Recommendation 3

We seek feedback about the relevance of the following potential supplemental Children's EHR Format requirements and their correlation to Recommendation 3.

1. *Title:* Ability to document parental (guardian) notification or permission.

Children's EHR Format: Req-2008: Release Package: 2015 Priority List.

Topic(s): Security and Confidentiality, Parents and Guardians, and Family Relationship Data.

Description: The system shall provide the ability to document parental (guardian) notification or permission for consenting minors to receive some treatments as required by institutional policy or jurisdictional law.

2015 Edition Criterion Alignment: Data segmentation for privacy—send criterion, data segmentation for privacy—receive criterion, and/or the patient health information capture criterion, view, download, and transmit (VDT) to third-party, and Application Programming Interface (API).

New or Updated Criterion Alignment: Data segmentation for privacy.

2. *Title:* Record parental notification of newborn screening diagnosis.

Children's EHR Format: Req-2016: Release Package: 2015 Priority List.

Topic(s): Newborn Screening.

Description: The system shall be able to track that the child's legal guardians were notified of any newborn screening-related diagnosis.

2015 Edition Criterion Alignment: Question: View, download, and transmit (VDT) to third-party, secure messaging, Application Programming Interface (API).

New or Updated Criterion Alignment: API.

3. *Title:* Authorized non-clinician viewers of EHR data.

Children's EHR Format: Req-2032—Release Package 2015 Priority List.

Topic(s): Child Welfare, Patient Portals (PHR).

Description: The system shall have the ability to identify members of the care team (including professional and nonprofessional members) and indicate their roles/relationships to the child.

2015 Edition Criterion Alignment: Care plan criterion, authentication, access control, and authorization.

New or Updated Criterion Alignment: API.

4. *Title:* Document decision-making authority of patient representative.

Children's EHR Format: Req-2030: Release Package: 2015 Priority List.

Topic(s): Security and Confidentiality.

Description: The system shall have the ability to store, retrieve, and display information about an individual's right to authorize care, to release information, and to authorize payment for care on behalf of the patient, including time restrictions or other limitations. This includes storing copies of the relevant consent and authorization forms in compliance with state and federal rules, and also includes cases of child foster care, state social services agencies, guardians, guarantors, and those recognized to have full or partial authority. The system shall allow for multiple individuals.

2015 Edition Criterion Alignment: Patient health information capture.

New or Updated Criterion Alignment: Data segmentation.

Recommendation 4: Segmented Access to Information

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Segmented access to information.

Children's EHR Format: Req-2041: Release Package: 2015 Priority List.

Topic(s): Security and Confidentiality.

Description: The system shall provide users the ability to segment health care data in order to keep information about minor consent services private and distinct from other content of the record, such that it is not exposed to parents/guardians without the minor's authorization.

Alignment With 2015 Edition Certification Criteria

ONC believes this recommendation is supported by the 2015 Edition Criteria listed below, and ONC believes this recommendation is supported by health IT beyond what is included in the certification program

- *Data Segmentation for Privacy* criteria:
  - ○ Data segmentation for privacy—send criterion provides the ability to create a summary record (formatted to Consolidated CDA (C–CDA) Release 2.1) that is tagged at the document level as restricted and subject to re-disclosure restrictions using the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.
  - ○ Data segmentation for privacy—receive criterion requires the ability to receive a summary record (formatted to Consolidated CDA Release 2.1) that is document—level tagged as restricted and subject to re-disclosure restrictions using the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1. Requires the ability to separate the document-level tagged document from other documents received. Requires the ability to view the restricted document without having to incorporate any of the data from the document.
- *Transitions of Care* criteria includes the ability to create, receive, and properly consumer interoperable documents using a common content and transport standard that include key health data that should be accessible and available for exchange.

Alignment With Proposed New or Updated Certification Criteria

ONC believes this recommendation is supported by the proposed new and updated certification criteria in this proposed rule:

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Data Segmentation for Privacy:* (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) would provide functionality to address the concerns multiple stakeholders expressed regarding the need to restrict granular pediatric health data at production based on the intended recipient of the data.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Supplemental Children's Format Requirements for Recommendation 4

We seek feedback about the relevance of the following potential Children's EHR Format requirements and their correlation to Recommendation 4.

1. *Title:* Problem-specific age of consent.

Children's EHR Format: Req-2039: Release Package: 2015 Priority List.

Topic(s): Security and Confidentiality.

Description: The system shall provide the ability to access legal guidelines on consent requirements for reference, where available, and to record the age of consent for a specific treatment when these differ based on legal guidelines.

2015 Edition Criterion Alignment: Demographics, care plan criterion, data segmentation for privacy—send, data segmentation for privacy—receive.

New or Updated Criterion Alignment: USCDI, data segmentation.

Recommendation 5: Synchronize Immunization Histories With Registries

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Synchronize immunization histories with registry.

Children's EHR Format: Req-2011*: Release Package: 2015 Priority List.

Topic(s): Registry Linkages, Immunizations.

Description: The system shall support updating and reconciling a child's immunization record with information received from immunization information systems or other health information exchanges (HIEs).

Title: Use established immunization messaging standards.

Children's EHR Format: Req-2028 Release Package: 2015 Priority List.

Topic(s): Registry Linkages, Immunizations.

Description: (A) The system shall use the messaging standards established through meaningful use requirements to send data to immunization information systems or other HIEs. (B) The system shall use the messaging standards established through meaningful use requirements to receive data from immunization information systems or other HIEs.

Alignment With 2015 Edition Certification Criterion

ONC believes this recommendation is supported by the 2015 Edition Criterion listed below:

- *Transmission to Immunization Registries* criterion, which:
  - ○ Provides the ability to create immunization information according to the implementation guide for Immunization Messaging Release 1.5, and the July 2015 addendum, using CVX codes for historical vaccines and NDC codes for newly administered vaccines.
  - ○ Provides the ability to request, access, and display the evaluated immunization history and forecast from an immunization registry for a patient in accordance with the HL7 2.5.1 standard, the HL7 2.5.1. IG for Immunization Messaging, Release 1.5, and July 2015 addendum.
- *View, Download, and Transmit to Third Party (VDT)* criterion, which:
  - ○ Provides the ability for patients (and their authorized representatives) to view, download, and transmit their health information to a third party via internet-based technology consistent with one of the Web Content Accessibility Guidelines (WCAG) 2.0 Levels A or AA.
  - ○ Requires the ability for patients (and their authorized representatives) to view, at a minimum, the Common Clinical Data Set, laboratory test report(s), and diagnostic image reports.

Alignment With Proposed New or Updated Certification Criteria

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Supplemental Children's Format Requirements for Recommendation 5

We seek feedback about the relevance of the following potential Children's EHR Format requirements and their correlation to Recommendation 5.

1. *Title:* Produce completed forms from EHR data.

The Children's EHR Format: Req-2027 Release Package: 2015 Priority List.

Topic(s): Well Child/Preventive Care, Immunizations.

Description: The system shall produce reports (*e.g.,* for camp, school, or child care) of a child's immunization history, including the following elements: Child's name, date of birth and sex, date the report was produced, antigen administered, date administered, route of administration (when available), and an indication of whether a vaccine was refused or contraindicated.

2015 Edition Certification Alignment: Transmission to immunization registries, View, Download and Transmit (VDT), Application Programming Interface (API).

New or Updated Criterion Alignment: API.

Recommendation 6: Age- and Weight-Specific Single-Dose Range Checking

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirements as follows:

Title: Age- and weight-specific single-dose range checking.

Children's EHR Format: Req-2037: Release Package: 2015 Priority List.

Topic(s): Medication Management.

Description: The system shall provide medication dosing decision support that detects a drug dose that falls outside the minimum-maximum range based on the patient's age, weight, and maximum recommended adult dose (if known) or maximum recommended pediatric dose (if known), for a single dose of the medication.

Alignment With 2015 Edition Certification Criteria

ONC believes this recommendation is supported by the 2015 Edition criterion listed below:

Clinical Decision Support (CDS) can be used to develop a variety of tools to enhance decision-making in the pediatric clinical workflow including contextually relevant reference information, clinical guidelines, condition-specific order sets, alerts, and reminders, among other tools.

Application Programming Interfaces criteria including the ''application access—patient selection'', ''application access—data category request'', and ''application access—all data request'' which can help address many of the challenges currently faced by caregivers accessing pediatric health data.

ONC believes this priority could also be supported by health IT beyond what is included in the certification program.

ONC notes that per the National Council for Prescription Drug Programs (NCPDP), dose-range checking should be based on industry drug database products and are not intrinsic to SCRIPT.

Alignment With Proposed New or Updated Certification Criteria

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Recommendation 7: Transferrable Access Authority

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Transferrable access authority.

Children's EHR Format: Req-2026: Release Package: 2015 Priority List.

Topic(s): School-Based Linkages, Security and Confidentiality, Patient Portals and Patient Health Records (PHR).

Description: The system shall provide a mechanism to enable access control that allows a transferrable access authority (*e.g.,* to address change in guardian, child reaching age of maturity, etc.).

Alignment With 2015 Edition Certification Criterion

ONC believes this recommendation is supported by the 2015 Edition criterion below.

- *View, Download, and Transmit to Third Party (VDT)* criterion, which:
  - ○ Provides the ability for patients (and their authorized representatives) to view, download, and transmit their health information to a third party via internet-based technology consistent with one of the Web Content Accessibility Guidelines (WCAG) 2.0 Levels A or AA.
  - ○ Requires the ability for patients (and their authorized representatives) to view, at a minimum, the Common Clinical Data Set, laboratory test report(s), and diagnostic image reports.

Application Programming Interfaces criteria including the ''application access—patient selection'', ''application access—data category request'', and ''application access—all data request'' which can help address many of the challenges currently faced by caregivers accessing pediatric health data.

Alignment With Proposed New or Updated Certification Criterion

- *Data Segmentation for Privacy:* (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) would provide functionality to address the concerns multiple stakeholders expressed regarding the need to restrict granular pediatric health data at production based on the intended recipient of the data.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Supplemental Children's Format Requirements for Recommendation 7

We seek feedback about the relevance of the following potential Children's EHR Format requirements and their correlation to Recommendation 7.

1. *Title:* Age of emancipation.

The Children's EHR Format: Requirement Req-2040 Release Package: 2015 Priority List.

Topic(s): Security and Confidentiality.

Description: The system shall provide the ability to record the patient's emancipated minor status.

2015 Edition Criterion Alignment: Demographic.

New or Updated Criterion Alignment: Data segmentation.

Recommendation 8: Associate Maternal Health Information and Demographics With Newborn

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Associate mother's demographics with newborn.

Children's EHR Format: Req-2021: Release Package: 2015 Priority List

Topic(s): Patient Identifier, Parents and Guardians and Family Relationship Data.

Description: The system shall provide the ability to associate identifying parent or guardian demographic information, such as relationship to child, street address, telephone number, and/or email address for each individual child.

Alignment With the 2015 Edition Certification Criterion

ONC believes this recommendation is supported by the 2015 Edition criterion below:

- *Care Plan:* Criteria includes the ability to record, change, access, create, and receive care plan information according to the care plan document template in the HL7 implementation guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), draft standard for Trial Use Release 2.1 (including the sections for health status evaluations and outcomes and for interventions (V2)).
- *Transitions of Care* criteria includes the ability to create and to receive interoperable documents using a comment content standard that include key health data that should be accessible and available for exchange to support the care of children across care settings.
- *Demographic* criterion requires the ability to record various demographic information for a patient including potential supports for patient and parental matching.
- *Family Health History* criterion permits the ability to record, change, and access a patient's family health history (according to the September 2015 release of SNOMED CT®, U.S. edition).
- *Social, Psychological, and Behavioral Data* criteria capture information (also known as social determinants of health) that can help to provide a more complete view of a mother's overall health status.

Alignment With Proposed New or Updated Certification Criteria

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Recommendation 9: Track Incomplete Preventative Care Opportunities

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Track incomplete preventive care opportunities.

Children's EHR Format: Req-2024: Release Package: 2015 Priority List.

Topic(s): Well Child/Preventive Care.

Description: The system shall generate a list on demand for any children who have missed recommended health supervision visits (*e.g.,* preventive opportunities), according to the frequency of visits recommended in Bright Futures™.

Alignment With 2015 Edition Certification Criteria

ONC believes this recommendation is supported by the 2015 Edition criterion below:

Clinical Decision Support (CDS) criterion includes configuration that enables interventions based on various CCDS data elements, including vital signs.

- *Clinical Quality Measures* criteria for record and export, import and calculate, and filter criteria:
  - ○ Record and export criterion ensures that health IT systems can record and export CQM data electronically; the export functionality gives clinicians the ability to export their results to multiple programs.
  - ○ import and calculate criterion supports streamlined clinician processes through the importing of CQM data in a standardized format and ensures that health IT systems can correctly calculate eCQM results using a standardized format.
  - ○ filter criterion supports the capability for a clinician to make a query for eCQM results using or a combination of data captured by the certified health IT for quality improvement and quality reporting purposes.
- *Application Programming Interfaces* criteria including the ''application access—patient selection'', ''application access—data category request'', and ''application access—all data request'' which can help address many of the challenges currently faced by caregivers accessing pediatric health data.

Alignment With Proposed New or Updated Certification Criteria

ONC believes this recommendation is supported by the proposed new and updated certification criteria in this proposed rule:

- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

Recommendation 10: Flag Special Health Care Needs

Alignment With Children's EHR Format

Stakeholders identified alignment with the Children's EHR Format Requirement as follows:

Title: Flag special health care needs.

The Children's EHR Format: Req-2014: Release Package: 2015 Priority List.

Topic(s): Children with Special Health Care Needs.

Description: The system shall support the ability for providers to flag or un-flag individuals with special health care needs or complex conditions who may benefit from care management, decision support, and care planning, and shall support reporting.

Alignment With 2015 Edition Certification Criteria

ONC believes this recommendation is supported by the 2015 Edition criterion below.

- *Problem List* criterion contains the patient's current health problems, injuries, chronic conditions, and other factors that affect the overall health and well-being of the patient.
- *Clinical Decision Support (CDS)* can be used to develop a variety of tools to enhance decision-making in the pediatric clinical workflow including contextually relevant

reference information, clinical guidelines, condition-specific order sets, alerts, and reminders, among other tools.

- *Clinical Quality Measures* criteria for record and export, import and calculate, and filter criteria:
  ○ Record and export criterion ensures that health IT systems can record and export CQM data electronically; the export functionality gives clinicians the ability to export their results to multiple programs.
  ○ import and calculate criterion supports streamlined clinician processes through the importing of CQM data in a standardized format and ensures that health IT systems can correctly calculate eCQM results using a standardized format.
  ○ filter criterion supports the capability for a clinician to make a query for eCQM results using or a combination of data captured by the certified health IT for quality improvement and quality reporting purposes.

Alignment With Proposed New or Updated Certification Criteria

ONC believes this recommendation is supported by the proposed new and updated certification criteria in this proposed rule:

- *United States Core Data for Interoperability (USCDI):* The USCDI (§ 170.213) which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference.
- *Application Programming Interfaces (APIs):* § 170.315(g)(10), would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications to establish standardized application programming interfaces (APIs) for interoperability purposes and to permit 3rd party software developers to connect to the electronic health record (EHR) through the certified API technology.

[FR Doc. 2019–02224 Filed 2–22–19; 4:15 pm]

BILLING CODE 4150–45–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

42 CFR Parts 406, 407, 422, 423, 431, 438, 457, 482, and 485

Office of the Secretary

45 CFR Part 156

[CMS–9115–P]

RIN 0938–AT79

Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers

AGENCY: Centers for Medicare & Medicaid Services (CMS), HHS.

ACTION: Proposed rule.

SUMMARY: This proposed rule is intended to move the health care ecosystem in the direction of interoperability, and to signal our commitment to the vision set out in the 21st Century Cures Act and Executive Order 13813 to improve access to, and the quality of, information that Americans need to make informed health care decisions, including data about health care prices and outcomes, while minimizing reporting burdens on affected plans, health care providers, or payers.

DATES: To be assured consideration, comments must be received at one of the addresses provided below, no later than 5 p.m. on May 3, 2019.

ADDRESSES: In commenting, please refer to file code CMS–9115–P. Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

Comments, including mass comment submissions, must be submitted in one of the following three ways (please choose only one of the ways listed):

1. *Electronically.* You may submit electronic comments on this regulation to *http://www.regulations.gov.* Follow the ‘‘Submit a comment’’ instructions.

2. *By regular mail.* You may mail written comments to the following address ONLY: Centers for Medicare & Medicaid Services, Department of Health and Human Services, Attention: CMS–9115–P, P.O. Box 8016, Baltimore, MD 21244–8016.

Please allow sufficient time for mailed comments to be received before the close of the comment period.

3. *By express or overnight mail.* You may send written comments to the following address ONLY: Centers for Medicare & Medicaid Services, Department of Health and Human Services, Attention: CMS–9115–P, Mail Stop C4–26–05, 7500 Security Boulevard, Baltimore, MD 21244–1850.

For information on viewing public comments, see the beginning of the **SUPPLEMENTARY INFORMATION** section.

FOR FURTHER INFORMATION CONTACT:

Alexandra Mugge, (410) 786–4457, for issues related to interoperability, CMS health IT strategy, technical standards and patient matching.

Natalie Albright, (410) 786–1671, for issues related to Medicare Advantage.

John Giles, (410) 786–1255, for issues related to Medicaid.

Emily Pedneau, (301) 492–4448, for issues related to Qualified Health Plans.

Meg Barry, (410) 786–1536, for issues related to CHIP.

Thomas Novak, (202) 322–7235, for issues related to trust exchange networks and payer to payer coordination.

Sharon Donovan, (410) 786–9187, for issues related to federal-state data exchange.

Daniel Riner, (410) 786–0237, for issues related to Physician Compare.

Ashley Hain, (410) 786–7603, for issues related to hospital public reporting.

Melissa Singer, (410) 786–0365, for issues related to provider directories.

CAPT Scott Cooper, USPHS, (410) 786–9465, for issues related to hospital and critical access hospital conditions of participation.

Lisa Bari, (410) 786–0087, for issues related to advancing interoperability in innovative models.

Russell Hendel, (410) 786–0329, for issues related to the Collection of Information or the Regulation Impact Analysis sections.

SUPPLEMENTARY INFORMATION:

Inspection of Public Comments: All comments received before the close of the comment period are available for viewing by the public, including any personally identifiable or confidential business information that is included in a comment. We post all comments received before the close of the comment period on the following website as soon as possible after they have been received: *http://www.regulations.gov.* Follow the search instructions on that website to view public comments.