DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General

42 CFR Parts 1003 and 1005

RIN 0936–AA09

Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules

AGENCY: Office of Inspector General (OIG), Department of Health and Human Services (HHS).

ACTION: Final rule.

SUMMARY: This final rule amends the civil money penalty (CMP) regulations of the Department of Health and Human Services (HHS) Office of Inspector General (OIG) to: incorporate new CMP authority for information blocking; incorporate new authorities for CMPs, assessments, and exclusions related to HHS grants, contracts, other agreements; and increase the maximum penalties for certain CMP violations.

DATES: This final rule is effective August 2, 2023, except for the additions of §§ 1003.1400, 1003.1410, and 1003.1420 (amendatory instruction 10), which are effective on September 1, 2023.

FOR FURTHER INFORMATION CONTACT: Robert Penezic, (202) 539–4021, *robert.penezic@oig.hhs.gov.*

SUPPLEMENTARY INFORMATION:

I. Executive Summary

A. Purpose and Need for Regulatory Action

This final rule implements three statutory provisions: (1) the amendment of the Public Health Service Act (PHSA), 42 U.S.C. 300jj–52, by the 21st Century Cures Act (Cures Act) authorizing OIG to investigate claims of information blocking and providing the Secretary of HHS (Secretary) authority to impose CMPs for information blocking; (2) the amendment of the Civil Monetary Penalties Law (CMPL), 42 U.S.C. 1320a–7a, by the Cures Act, Public Law 114–255, section 5003, authorizing HHS to impose CMPs, assessments, and exclusions upon individuals and entities that engage in fraud and other misconduct related to HHS grants, contracts, and other agreements (42 U.S.C. 1320a–7a(o)–(s)); and (3) the increase in penalty amounts in the CMPL effected by the Bipartisan Budget Act of 2018 (BBA 2018), Public Law 115–123. Each of these statutory amendments is discussed further below.

First, section 4004 of the Cures Act added section 3022 to the PHSA, 42 U.S.C. 300jj–52 which, among other provisions, provides OIG the authority to investigate claims of information blocking and authorizes the Secretary to impose CMPs against a defined set of individuals and entities that OIG determines committed information blocking. Investigating and taking enforcement action against individuals and entities that engage in information blocking are consistent with OIG's history of investigating serious misconduct that impacts HHS programs and beneficiaries. Information blocking poses a threat to patient safety and undermines efforts by providers, payers, and others to make the health system more efficient and effective. Information blocking may also constitute an element of a fraud scheme, such as by forcing unnecessary tests or conditioning information exchange on referrals. Addressing the negative effects of information blocking is consistent with OIG's mission to protect the integrity of HHS programs, as well as the health and welfare of program beneficiaries.

In this final rule, we implement section 3022(b)(2)(C) of the PHSA, which requires that the CMP for information blocking follow the procedures of section 1128A of the Social Security Act (SSA). Specifically, the final rule adds the information blocking CMP authority to the existing regulatory framework for the imposition and appeal of CMPs, assessments, and exclusions (42 CFR parts 1003 and 1005) pursuant to section 3022(b)(2)(C) of the PHSA (42 U.S.C. 300jj–52(b)(2)(C)). The amendments give individuals and entities subject to CMPs for information blocking the same procedural rights that currently exist under 42 CFR parts 1003 and 1005. Through this final rule, we codify this new information blocking authority at 42 CFR 1003.1400, 1003.1410, and 1003.1420.

The final rule also explains OIG's approach to enforcement, which will focus on information blocking allegations that pose greater risk to patients, providers, and health care programs, as well as OIG's anticipated consultation and coordination with the Office of the National Coordinator for Health Information Technology (ONC) and other agencies, as appropriate, in reviewing and investigating allegations of information blocking.

On May 1, 2020, ONC published a final rule, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (ONC Final Rule), in the **Federal Register**. 85 FR 25642, May 1, 2020. Among other things, ONC through the ONC Final Rule promulgated the information blocking regulations defining information blocking and establishing exceptions to that definition. OIG's final rule incorporates the relevant information blocking regulations at 45 part 171 as the basis for imposing CMPs for information blocking.

Second, this final rule modifies 42 CFR parts 1003 and 1005 to add the new authority related to fraud and other misconduct involving grants, contracts, and other agreements into the existing regulatory framework for the imposition and appeal of CMPs, assessments, and exclusions. The additions: (1) expressly enumerate in the regulation the grant, contract, and other agreement fraud and misconduct CMPL authority; and (2) give individuals and entities sanctioned for fraud and other misconduct related to HHS grants, contracts, and other agreements the same procedural and appeal rights that currently exist under 42 CFR parts 1003 and 1005 for those sanctioned under the CMPL and other statutes for fraud and other misconduct related to, among other things, the Federal health care programs. In this final rule, we codify these new authorities and their corresponding sanctions in the regulations at 42 CFR 1003.110, 1003.130, 1003.140, 1003.700, 1003.710, 1003.720, 1003.1550, 1003.1580, and 1005.1.

On February 9, 2018, the President signed into law the BBA 2018. Section 50412 of the BBA 2018 amended the CMPL to increase the amounts of certain CMPs. 42 U.S.C. 1320a–7a(a), (b). This final rule codifies the increased CMPs at 42 CFR part 1003. Specifically, for conformity with the CMPL as amended by the BBA 2018, we revise the CMPs contained at 42 CFR 1003.210, 1003.310, and 1003.1010.

B. Legal Authority

The legal authority for this regulatory action is found in the SSA and the PHSA, as amended by the Cures Act and the BBA 2018. The legal authority for the changes is listed by the parts of title 42 of the Code of Federal Regulations (CFR) that we propose to modify:

1003: 42 U.S.C. 1320a–7a(a)–(b), (o)–(s); 42 U.S.C. 300jj–52

1005: 42 U.S.C. 1320a–7a(o)–(s); 42 U.S.C. 300jj–52

C. Proposed Rule

On April 24, 2020, OIG published a proposed rule (proposed pule) in the **Federal Register** setting forth certain proposed amendments to the CMP rules of HHS OIG. 85 FR 22979, April 24, 2020. The proposed rule set forth

proposed regulations that would: (1) incorporate the new CMP authority for information blocking; (2) incorporate new authorities for CMPs, assessments, and exclusions related to HHS grants, contracts, other agreements; and (3) increase the maximum penalties for certain CMP violations. We solicited comments on those three proposed regulatory additions and changes to obtain public input. Specific to information blocking, we also provided information on—but did not propose regulations for—our expected enforcement priorities, the investigation process, and our experience with investigating conduct that includes an intent element. We received 49 timely comments, 48 of which were unique, from a broad range of stakeholders.

D. Final Rule

This final rule incorporates into OIG's CMP regulations at 42 CFR parts 1003 and 1005 two new CMP authorities established by the Cures Act related to: (1) information blocking; and (2) fraud and other misconduct involving HHS grants, contracts, and other agreements. The final rule also incorporates into 42 CFR part 1003 new maximum CMP amounts for certain offenses, as set by the BBA 2018.

In the context of information blocking, the Cures Act authorizes CMPs for any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI) if the practice is conducted by an entity that is: a developer of certified health information technology (IT); offering certified health IT; a health information exchange (HIE); or a health information network (HIN) and the entity knows or should know that the practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI.

The ONC Final Rule implements certain Cures Act information blocking provisions, including defining terms and establishing reasonable and necessary activities that do not constitute information blocking or ''exceptions'' to the definition of information blocking. OIG and ONC have coordinated extensively on the ONC Final Rule and this final rule to align both sets of regulations. As proposed, we incorporate the regulatory definitions and exceptions in ONC's regulations at 45 CFR part 171 related to information blocking as the basis for imposing CMPs and determining the amount of penalty imposed.

In the context of HHS grants, contracts, and other agreements, the Cures Act authorizes CMPs, assessments, and exclusions for:

- knowingly presenting or causing to be presented a specified claim under a grant, contract, or other agreement that a person knows or should know is false or fraudulent;
- knowingly making, using, or causing to be made or used any false statement, omission, or misrepresentation of a material fact in any application, proposal, bid, progress report, or other document that is required to be submitted in order to directly or indirectly receive or retain funds provided in whole or in part by HHS pursuant to a grant, contract, or other agreement;
- knowingly making, using, or causing to be made or used, a false record or statement material to a false or fraudulent specified claim under a grant, contract, or other agreement;
- knowingly making, using, or causing to be made or used, a false record or statement material to an obligation to pay or transmit funds or property to HHS with respect to a grant, contract, or other agreement;
- knowingly concealing or knowingly and improperly avoiding or decreasing an obligation to pay or transmit funds or property to HHS with respect to a grant, contract, or other agreement; and
- failing to grant timely access, upon reasonable request, to OIG for the purposes of audits, investigations, evaluations, or other statutory functions of OIG in matters involving grants, contracts, or other agreements.

We further codify changes to the CMP regulations at 42 CFR part 1003 to conform with the CMP amounts contained in the SSA, as amended by the BBA 2018.

II. Background

For more than 35 years, OIG has exercised authority to impose CMPs, assessments, and exclusions in furtherance of its mission to protect Federal health care and other Federal programs from fraud, waste, and abuse. The Cures Act established new CMP authorities related both to information blocking and to fraud and other prohibited conduct involving HHS grants, contracts, and other agreements. OIG also received authority through the BBA 2018 to impose larger CMPs for certain offenses committed after February 9, 2018.

A. Overview of OIG Civil Money Penalty Authorities

The CMPL (section 1128A of the SSA, 42 U.S.C. 1320a–7a) was enacted in 1981 to provide HHS with the statutory authority to impose CMPs, assessments, and exclusions upon persons who commit fraud and other misconduct related to Federal health care programs, including Medicare and Medicaid. The Secretary delegated the CMPL's authorities to OIG. 53 FR 12993, April 20, 1988. HHS has promulgated regulations at 42 CFR parts 1003 and 1005 that: (1) enumerate specific bases for the imposition of CMPs, assessments, and exclusion under the CMPL and other CMP statutes; (2) set forth the appeal rights of persons subject to those sanctions; and (3) outline the procedures under which a sanctioned party may appeal the sanction. Since 1981, Congress has created various other CMP authorities related to fraud and abuse that were delegated by the Secretary to OIG and added to part 1003.

B. The Cures Act and the ONC Final Rule

The Cures Act added section 3022 of the PHSA, which defines conduct that constitutes information blocking by health IT developers of certified health IT, entities offering certified health IT, HIEs, HINs, and health care providers. Section 3022(a) of the PHSA defines information blocking as a practice that—(A) except as required by law or specified by the Secretary pursuant to rulemaking under section 3022(a)(3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and (B)(i) if conducted by a health information technology developer, exchange, or 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 (ii) 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. Section 3022(a)(3) of the PHSA provides that the Secretary shall, through rulemaking, identify reasonable and necessary activities that do not constitute information blocking, and section 3022(a)(4) of the PHSA states that the term ''information blocking'' does not include any conduct that occurred before January 13, 2017. The ONC Final Rule implements these sections of the PHSA at 45 CFR part 171.

Section 3022(b)(1) of the PHSA authorizes OIG to investigate claims of information blocking described in section 3022(a) of the PHSA, and to investigate claims that health IT developers of certified health IT or other

entities offering certified health IT have submitted false attestations under section 3001(c)(5)(D) of the PHSA as part of ONC's program for the voluntary certification of health IT (ONC Health IT Certification Program). Section 3022(b)(2)(A) authorizes the Secretary to impose CMPs not to exceed $1 million per violation on health IT developers of certified health IT or other entities offering certified health IT, HIEs, and HINs that OIG determines, following an investigation, committed information blocking. Section 3022(b)(2)(A) also provides that a determination of the CMP amounts shall consider factors such as the nature and extent of the information blocking and harm resulting from such information blocking including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted. Section 3022(b)(2)(C) of the PHSA applies the procedures of section 1128A of the SSA to CMPs imposed under section 3022(b)(2) of the PHSA in the same manner as such provisions apply to a CMP or proceeding under section 1128A(a) of the SSA. This final rule implements section 3022(b)(2)(A) and (C) of the PHSA.

Furthermore, section 3022(b)(2)(B) of the PHSA provides that any health care provider determined by 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 of HHS sets forth through notice and comment rulemaking. This final rule does not implement section 3022(b)(2)(B) of the PHSA. However, a health IT developer of certified health IT, HIE, or HIN as defined in 45 CFR 171.102 determined by OIG to have committed information blocking could be subject to CMPs under this final rule even if that entity also met the definition of a health care provider at 45 CFR 171.102. For additional discussion related to health care providers that meet a definition of an actor subject to CMPs, see section IV.A.3. of this preamble.

The Cures Act also identifies ways for ONC, the Office for Civil Rights (OCR), and OIG to consult, refer, and coordinate. For example, section 3022(b)(3) of the PHSA states that OIG may refer instances of information blocking to OCR when a consultation regarding the health privacy and security rules promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will resolve such information blocking claims. Additionally, section 3022(d)(1) of the PHSA requires ONC to share information with OIG as required by law. For additional discussion related to coordination, see section III.A.5 of the proposed rule preamble and section III.B. of this preamble.

ONC's information blocking regulations at 45 CFR part 171 and the OIG CMP regulation at 42 CFR part 1003, subpart N, are designed to work in tandem. As a result, we encourage parties to read this final rule together with the ONC Final Rule. The ONC Final Rule defined ''information blocking''—and specific terms related to information blocking—as well as implemented exceptions to the definition of information blocking. This final rule describes the parameters and procedures applicable to the CMP for information blocking.

The Cures Act amended the CMPL to give HHS the authority to impose CMPs, assessments, and exclusions upon persons that commit fraud and other misconduct related to HHS grants, contracts, and other agreements. 42 U.S.C. 1320a–7a(o)–(s). This authority allows for the imposition of sanctions for a wide variety of fraudulent and improper conduct involving HHS grants, contracts, and other agreements including, among other things, the making of false or fraudulent specified claims to HHS, the submission of false or fraudulent documents to HHS, and the creation of false records related to HHS grants, contracts, or other agreements. The authority applies to a broad array of situations in which HHS provides funding, directly or indirectly, in whole or in part, pursuant to a grant, contract, or other agreement. The Cures Act also created a new set of definitions related to grant, contract, and other agreement fraud and misconduct, outlined the sanctions for violation of the statute, and referenced the procedures to be used when imposing sanctions under the statute.

C. The Bipartisan Budget Act of 2018

The BBA 2018 amended the CMPL to increase certain CMP amounts contained in 42 U.S.C. 1320a–7a(a) and (b). The BBA 2018 increased the maximum CMP amounts in section 1128A(a) of the SSA (42 U.S.C. 1320a–7a) from $10,000 to $20,000; from $15,000 to $30,000; and from $50,000 to $100,000. The BBA 2018 increased the maximum CMP amounts in section 1128A(b) of the SSA from $2,000 to $5,000 in paragraph (1), from $2,000 to $5,000 in paragraph (2), and from $5,000 to $10,000 in paragraph (3)(A)(i). This statutory increase in CMP amounts is effective for acts committed after the date of enactment, February 9, 2018. This final rule updates our regulations to reflect the increased CMP amounts authorized by the 2018 BBA amendments.

III. OIG's Anticipated Approach to Information Blocking CMP Enforcement

The preamble to the proposed rule provided a nonbinding, informational overview of our anticipated information blocking enforcement priorities and the investigative process. We provided this information in the preamble to the proposed rule for informational purposes only and did not propose regulations on these topics. We received several comments on these topics, which are publicly available at *https://www.regulations.gov/docket/HHSIG-2020-0001/comments.* To improve public understanding of how we anticipate we will approach information blocking CMP enforcement, we further provide in section III of this preamble an informational statement to supplement the discussion set forth in the proposed rule. We note that this discussion of anticipated approach is limited to our investigation of those entities subject to CMPs and does not apply to the investigation of health care providers that may be referred for disincentives under section 3022(b)(2)(B) of the PHSA.

A. Anticipated Priorities

The preamble to the proposed rule set forth our anticipated information blocking enforcement priorities as conduct that: (1) resulted in, is causing, or had the potential to cause patient harm; (2) significantly impacted a provider's ability to care for patients; (3) was of long duration; (4) caused financial loss to Federal health care programs, or other government or private entities; or (5) was performed with actual knowledge. We explained that we will select cases for investigation based on these priorities and expect that the enforcement priorities will evolve as OIG gains more experience investigating information blocking. We also emphasized that the definition of information blocking—as defined in section 3022(a) of the PHSA and 45 CFR 171.103(a)—includes an element of intent and that OIG lacked the authority to seek CMPs for information blocking against actors who did not have the requisite intent. We continue to anticipate the same enforcement priorities as set out in the preamble of the proposed rule and supplement that discussion below. We provide this explanation so that the public and stakeholders have a better understanding of how we anticipate allocating our resources to enforce the

CMP for information blocking. Prioritization ensures OIG can effectively allocate its resources to target information blocking allegations that have more negative effects on patients, providers, and health care programs. Our enforcement priorities will inform our decisions about which information blocking allegations to pursue, but these priorities are not dispositive. Each allegation will present unique facts and circumstances that must be assessed individually. Each allegation will be assessed to determine whether it implicates one or more of the enforcement priorities, or otherwise merits further investigation and potential enforcement action. There is no specific formula we can apply to every allegation that allows OIG to effectively evaluate and prioritize which claims merit investigation.

As addressed in section III.B of this preamble, we anticipate coordinating closely with ONC and other agencies as appropriate in reviewing allegations. Although our statement of anticipated priorities is framed around individual allegations, OIG may evaluate allegations and prioritize investigations based in part on the volume of claims relating to the same (or similar) conduct by the same actor. That evaluation would include assessment of all information blocking claims received by ONC through the standardized process to receive claims from the public.

We clarify here that OIG's anticipated priority relating to patient harm is not specific to individual harm, but rather may broadly encompass harm to a patient population, community, or the public. Additionally, with respect to our anticipated priority relating to actual knowledge, we note that health IT developers of certified health IT and health information exchanges and networks do not have to have actual knowledge in order to commit information blocking. But the conduct of someone who has actual knowledge is generally more egregious than the conduct of someone who only should know that their practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. As a general matter, we would likely prioritize cases in which an actor has actual knowledge over cases in which the actor only should have known that the practice was likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI.

Finally, we are stating that our current anticipated enforcement priorities may lead to investigations of anti-competitive conduct or unreasonable business practices. The ONC Final Rule provides, as examples, conduct that may implicate the information blocking provision, anti-competitive or unreasonable conduct, such as unconscionable or one-sided business terms for the access, exchange, or use of EHI, or the licensing of an interoperability element. For example, a contract containing unconscionable terms related to sharing of patient data could be anti-competitive conduct that impedes a provider's ability to care for patients. 85 FR 25812, May 1, 2020. A claim of such conduct would implicate OIG's enforcement priority related to a provider's ability to care for patients. Anti-competitive conduct resulting in information blocking could implicate other enforcement priorities as well, depending on the facts.

OIG's enforcement priorities are a tool we use to triage allegations and allocate resources. We can and do expect to investigate allegations of other information blocking conduct not covered by the priorities. If conduct or patterns of conduct raise concerns, OIG may choose to investigate those allegations. And as we gain more experience with investigating information blocking, we will reassess our priorities accordingly. For example, as patients continue to adopt and use technology to access their EHI, the number of patients that will request their EHI directly from a health IT developer of certified health IT or HIE may increase. That may generate more allegations related to patient access to their EHI. Trends or changes in the types of allegations we receive may affect enforcement priorities in the future.

B. Coordination With Other Agencies

The Cures Act identified ways for ONC, OCR, and OIG to consult, refer, and coordinate on information blocking claims. We elaborate on those processes here for informational purposes only.

Section 3022(d)(1) of the PHSA states that ONC may serve as a technical consultant to OIG. Because ONC promulgated the information blocking regulations and exceptions, OIG will closely consult with ONC throughout the investigative process. ONC's subject matter expertise is vital to our evaluation of information blocking allegations. OIG will continue working closely with ONC as ONC develops information blocking guidance.

Section 3022(d)(3) of the PHSA requires ONC to implement a standardized process for the public to submit reports on claims of information blocking, and section 3022(d)(1) requires ONC to share information with OIG as required by law. ONC has a standardized process for the public to submit reports on claims of information blocking through this website: *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/6*. In addition to the process required by the PHSA, OIG has its own hotline process through which individuals may submit claims of information blocking online at *https://tips.oig.hhs.gov/* or by calling 1–800–447–8477. Regardless of whether a claim is made to ONC or OIG, ONC and OIG will coordinate in evaluating claims of information blocking and share information as permitted by law.

Whether OIG's or ONC's authority is appropriate to address a claim of information blocking will depend on the facts and circumstances of the allegation and the results of an investigation. For example, ONC and OIG may initially agree that a claim is most appropriately evaluated through an OIG investigation. ONC has authority to take action against an individual or entity that is a developer participating in the ONC Health IT Certification Program. 45 CFR 170.580. OIG has authority to impose CMPs against a health IT developer of certified health IT, which includes developers participating in the ONC Health IT Certification Program. Thus, an individual or entity that meets the definition of health IT developer of certified health IT could be subject to CMPs, termination of certification or other action under the ONC Health IT Certification Program review process, or both. 85 FR 25789, May 1, 2020.

In addition to coordination with ONC, section 3022(b)(3) of the PHSA provides the option for OIG to refer instances of information blocking to OCR when a consultation regarding the health privacy and security rules promulgated under section 264(c) of HIPAA will resolve such information blocking claims. Depending on the facts and circumstances of an information blocking claim, OIG will exercise this statutory discretion as appropriate to refer persons to consult with OCR to resolve information blocking claims. There is no set of facts or circumstances that will always be referred to OCR. OIG will work with OCR to determine which claims should be referred to OCR under the new authorities found in section 3022(b)(3) of the PHSA. In addition to section 3022(b)(3), OIG may request technical assistance from OCR during an information blocking investigation. OIG may also refer to OCR claims of information blocking that would be better resolved under OCR's HIPAA authorities.

Specific to anti-competitive conduct, we note that section 3022(d) of the PHSA includes specific options for ONC

and OIG to coordinate with the Federal Trade Commission (FTC) related to an information blocking claim. Under section 3022(d)(1) of the PHSA, ONC may share information related to claims of information blocking or investigations by OIG with the FTC for purposes of such investigation. We will coordinate closely with ONC to identify claims and investigations or patterns of claims and investigations that may warrant referral to the FTC.

We further note that following our investigation and the imposition of CMPs, our coordination with ONC, OCR, or other agencies as relevant may continue as part of an appeal of the imposition of CMPs by OIG. Upon the issuance of a notice of proposed determination for a CMP in accordance with 42 CFR 1003.1500, the actor may appeal the proposed determination for a CMP in accordance with the appeal procedures set forth in 42 CFR part 1005. As noted in 42 CFR 1005.2(a), a party sanctioned under any criteria in 42 CFR part 1003 may request a hearing before an administrative law judge (ALJ). 42 CFR 1005.2. The facts of the matter under appeal will determine the specific agencies with which we may coordinate.

We also anticipate coordinating with other HHS agencies to avoid duplicate penalties. Section 3022(d)(4) of the PHSA requires that the Secretary, to the extent possible, ensure that penalties do not duplicate penalty structures that would otherwise apply to information blocking and the type of individual or entity involved as of the day before the enactment of the Cures Act, December 13, 2016. Depending on the facts and circumstances, OIG might also consult or coordinate with a range of other agencies that might have relevant information or be able to provide technical assistance, including the Centers for Medicare and Medicare Services (CMS), other HHS agencies, FTC, or others. We discuss what enforcement coordination may look like in section III.D of the preamble.

C. Anticipated Enforcement Approach

Some commenters expressed interest in understanding OIG's enforcement approach, including: (1) whether OIG would include alternative actions, in lieu of the imposition of CMPs, such as providing actors subject to CMPs with additional education or corrective action plans; (2) whether OIG's approach to information blocking investigations would include investigating potential non-compliance with the requirements of CMS's Promoting Interoperability Program for eligible hospitals and critical access hospitals (CAHs) and Merit-based Incentive Payment System (MIPS) promoting interoperability performance category for clinicians; (3) whether actors may be subject to False Claims Act (FCA) liability for engaging in conduct that constitutes information blocking; and (4) whether OIG plans to create a self-disclosure protocol (SDP).

At this point, we do not anticipate using alternatives to CMPs as described by the commenters. OIG will have an SDP to resolve CMP liability and allow for lower penalties. As we gain more experience investigating and imposing CMPs for information blocking, we may further consider alternative enforcement approaches. HHS or OIG may also consider issuance of compliance guidance or other educational materials on the topic of information blocking.

OIG's historical position in its administrative enforcement under the CMPL is that the Federal health care programs are best protected when persons who engage in fraudulent or other improper conduct are assessed a financial sanction. This remedial purpose is at the core of OIG's administrative enforcement authorities.

The PHSA and existing regulatory structures provide options for ONC and OCR to conduct individualized education and corrective action plans when an actor has committed information blocking, and OIG may refer matters to ONC or OCR for such actions. For example, OIG may refer an allegation to OCR for consultation regarding the health privacy and security rules or for OCR to address under its HIPAA authorities. Similarly, OIG may refer an allegation to ONC to address under its direct review authority, under which ONC could impose a corrective action plan. ONC also stated in the ONC Final Rule that ONC's and OIG's respective authorities are independent and that either office may exercise its authority at any time. 85 FR 25789, May 1, 2020. Thus, OIG's enforcement action will only include a CMP, while ONC could purse a separate enforcement action within its authority, which could include a corrective action plan.

As noted above, this rulemaking does not address OIG investigations of potential information blocking by healthcare providers. HHS is developing a separate notice of proposed rulemaking to establish appropriate disincentives for healthcare providers as described in the Unified Agenda at *https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=0955-AA05.* However, in response to commenters' inquiry we clarify that OIG does not intend to use its authority to investigate information blocking under section 3022(b)(1) of the PHSA to investigate potential non-compliance with CMS programmatic requirements, including those under the Promoting Interoperability Program for eligible hospitals and CAHs and MIPS promoting interoperability performance category for clinicians, that are distinct from the information blocking provisions of the PHSA. If investigations into alleged information blocking suggest a health care provider may be out of compliance with CMS programmatic requirements, OIG may refer such matters to CMS.

Similarly, conduct that constitutes information blocking could create false claims liability for an actor. For example, by engaging in conduct that constitutes information blocking, a health IT developer of certified health IT may have falsified attestations made to ONC as part of the ONC Health IT Certification Program. By falsifying its attestation, the health IT developer of certified health IT may cause health care providers to file false attestations under MIPS. Such a fact-specific determination would be assessed in coordination with OIG's law enforcement partners, including the Department of Justice.

Information blocking is newly regulated conduct, and OIG has not created an SDP specifically for information blocking; however, after the publication of this rule, OIG will add an information blocking SDP, including an online submission form, and other processes, to OIG's existing SDP located at *https://oig.hhs.gov/compliance/self-disclosure-info/.*

We understand many stakeholders may not be familiar with OIG's current SDP and provide the following information regarding the forthcoming information blocking SDP and self-disclosure process. The information blocking SDP will provide actors with a framework and mechanism for evaluating, disclosing, coordinating, and resolving CMP liability for conduct that constitutes information blocking. When posted on our website, OIG's SDP will explain: (1) eligibility criteria, (2) manner and format, (3) required contents of a submission, and (4) expected resolution of the matter. The information blocking SDP will be available only to those actors seeking to resolve potential CMP liability.

We recognize that whether to disclose potential information blocking violations to OIG is a significant decision; however, the significant benefits to disclosing potential information blocking violations to OIG should make that decision easier. First,

actors accepted by OIG into the SDP who cooperate with OIG during the self-disclosure process will pay lower damages than would normally be required in resolving a government-initiated investigation. Second, through our experience with OIG's existing SDP, we know that self-disclosure provides the opportunity for an actor to avoid costs and disruptions associated with government-directed investigations and civil or administrative litigation. Finally, OIG created the original SDP to provide a consistent, specific, and detailed process that can be relied upon by all participants, and we are similarly committed to working with actors that use the SDP in good faith to disclose information blocking conduct and cooperate with OIG's review and resolution process.

We reiterate that self-disclosing conduct is for an actor to resolve its own potential liability under the CMP for information blocking. It would not resolve any liability an actor may have under other applicable law, such as under HIPAA or under the ONC Certification Program. Actors should not self-disclose to seek opinions from OIG as to whether an individual or entity meets the definitions of a ''health IT developer of certified health IT'' or ''health information network or health information exchange'' in 45 CFR 171.102 or whether conduct constitutes information blocking under section 3022(a) of the PHSA and corresponding implementing regulations. Actors seeking to inform OIG about another individual's conduct should use the ONC portal or the OIG hotline.

As mentioned above, OIG will provide additional information on our website regarding the SDP for information blocking after publication of this final rule. However, before such information is posted, OIG will accept self-disclosure of information blocking conduct. We refer actors to section IV.A.5 of the preamble that describes how we will evaluate disclosure of violations and cooperation with investigations.

Specifically, it is a mitigating circumstance under the factors at 42 CFR 1003.140(a)(2) for an actor to take appropriate and timely corrective action in response to a violation. Timely corrective action includes disclosing information blocking violations to OIG and fully cooperating with OIG's review and resolution of such disclosure.

D. Advisory Opinions

Some commenters requested that OIG develop an advisory opinion process for individuals and entities to obtain advisory opinions on whether specified conduct constitutes information blocking for which OIG may impose a CMP. Pursuant to section 1128D(b) of the SSA, HHS, through OIG, publishes advisory opinions regarding the application of the Federal anti-kickback statute and the associated safe harbor provisions, as well as specified administrative sanction authorities, to proposed or existing arrangements. Section 1128D(b) specifies the matters subject to advisory opinions under that authority. The CMP for information blocking is not one of the administrative sanction authorities specified by section 1128D(b) of the SSA.

Furthermore, the Cures Act did not establish an advisory opinion process with regard to the application of OIG's information blocking-related administrative enforcement authorities. At present, OIG has no plans to develop and establish an advisory opinion process regarding the application of the CMP for information blocking. The Justification of Estimates to the Appropriations Committee for the President's fiscal year (FY) 2024 budget included a legislative proposal to provide HHS the authority to issue advisory opinions on information blocking practices.

IV. Summary of Final Rule Provisions, Public Comments, and OIG Response

A. The CMP for Information Blocking

As a general matter, commenters were supportive of OIG's proposed information blocking rules but sought more information and guidance from both ONC and OIG. Commenters suggested that the effective date for the CMP for information blocking rules be delayed as a result of the ongoing public health emergency (PHE) due to SARS–CoV–2, which causes COVID–19, and the requests for additional guidance from ONC and OIG. Many commenters sought clarification on the ONC Final Rule, such as whether an individual or entity falls within the category of actors that OIG would subject to CMPs for information blocking. Many commenters requested that OIG, either in this final rule or through guidance, further elaborate on and provide examples of how OIG will determine violations and CMP amounts. We have considered these comments carefully in developing the final rule, as described in more detail in responses to comments.

1. Information Blocking CMP Regulatory Authority & CMP Process

We proposed to add the CMP for information blocking to our existing CMP regulations at 42 CFR part 1003 and to apply the existing procedural and appeal rights at 42 CFR parts 1003 and 1005 to the CMP for information blocking. We solicited comment on the proposed application of the existing CMP procedures and appeal process in parts 1003 and 1005 to the CMP for information blocking. Commenters were generally in favor of incorporating the CMP for information blocking into these sections and applying the existing appeal processes set forth at 42 CFR part 1005. In this rule, we finalize the addition of the CMP for information blocking to 42 CFR part 1003 and the application of parts 1003 and 1005 to the CMP for information blocking as proposed without modification.

We also proposed to add the authority for OIG's imposition of CMPs for information blocking (section 3022 of the PHSA, 42 U.S.C. 300jj–52) to the list of statutory CMP provisions that appears in 42 CFR 1003.100. We received no comment on this proposed change and finalize the rule as proposed without modification.

Comment: One commenter believed that the application of 42 CFR 1005.7 to the CMP for information blocking was unworkable in its current form. The commenter believed that the discovery process under 42 CFR 1005.7 as currently written was inconsistent with the Cures Act's intent for ONC, OCR, and OIG to consult, refer, and coordinate in the investigation and enforcement of investigation blocking. The commenter further stated that, consistent with the prior OIG final rule, Amendments to the OIG Exclusion and CMP Authorities Resulting From Public Law 100–93, 57 FR 3325, January 29, 1992, OIG would only be required to produce documents in its possession and not documents in the possession of other branches or divisions of HHS. The commenter further believed 42 CFR 1005.7 as written would prohibit individuals and entities that appeal the imposition of CMPs for information blocking from obtaining relevant documentary evidence maintained in ONC's possession. The commenter also believed that OIG could abuse the discovery process by refusing to take ''possession'' of documents in ONC's care, custody, or control in an effort to avoid producing them. The commenter further believed that, as ONC would not be covered by the discovery rule at 42 CFR 1005.7, ONC would not be subject to any document preservation requirement that would increase the potential for the spoliation or destruction of evidence.

Response: We did not propose revising—and this final rule does not make revisions to—42 CFR 1005.7. The

CMP for information blocking appeals will be subject to discovery rules in 42 CFR 1005.7 because the Cures Act requires OIG to follow existing CMP procedures. Section 3022(b)(2)(C) of the PHSA requires the CMP for information blocking to follow procedures of section 1128A of the SSA, and 42 CFR part 1005 implements those procedures. Therefore, applying the procedures at 42 CFR part 1005 to CMP for information blocking appeals is consistent with the Cures Act.

We appreciate that the CMP appeals process and the discovery provided therein may be new for many actors subject to CMPs for information blocking, and we further elaborate below.

Whenever we propose to impose CMPs for information blocking, the actor will have the opportunity to appeal the CMPs. That appeal will be heard by an administrative law judge (ALJ) and governed by the procedures set forth in 42 CFR part 1005. The regulation at 42 CFR 1005.7 addresses discovery and allows each party to request that the other party produce nonprivileged documents that are relevant and material to the issues before the ALJ for inspection and copying. If the other party objects to producing the requested documents, the party requesting the documents can ask the ALJ to compel discovery.

The discovery regulations that will apply to appeals of CMPs for information blocking are the same regulations that have applied to existing CMPL administrative litigation. These regulations and this process have been approved by administrative tribunals and Federal courts. We provide limited discovery in our CMP cases even though it is not required in administrative proceedings at all. 57 FR 3298, January 29, 1992. The regulation at 42 CFR 1005.7 limits discovery to the exchange of material and relevant documents to avoid the time-consuming discovery fights that can affect civil litigation. Additionally, the vast bulk of material and relevant evidence (*i.e.,* evidence relating to whether the actor committed information blocking) will come from the actor whose conduct is at issue and not the government.

In addition to the specific discovery rules in 42 CFR 1005.7, there are other provisions in 42 CFR part 1005 that ensure transparency and fairness in an appeal. For example, 42 CFR 1005.8 calls for the parties to exchange witness lists, copies of prior written statements of proposed witnesses, and copies of proposed hearing exhibits. If OIG proposed to use documents or testimony from ONC or other government agencies as evidence in support of the imposition of CMPs, those exhibits and statements would be made available under 42 CFR 1005.8.

Regarding the commenter's specific concern that 42 CFR 1005.7 is not consistent with the coordination with ONC and OCR suggested by the Cures Act, we do not agree. The Cures Act provides OIG the discretionary authority to coordinate or consult with ONC and OCR, as necessary. For example, under section 3022(b)(3)(A) of the PHSA, OIG ''may refer'' instances of information blocking to OCR if we determine that consulting with OCR may resolve an information blocking claim. While not required, we expect that nearly all information blocking investigations will be done in coordination with ONC. This close coordination with another HHS agency is not unique to information blocking or the Cures Act. Many of our CMP cases involve similarly close coordination with CMS, for example. There is nothing unique to the Cures Act that would necessitate a change from our current discovery procedures.

We do not agree with the commenter's concerns about spoliation or destruction of documents in ONC's possession. ONC would not be a party to discovery in a CMP for information blocking matter, so the concept of spoliation—at least as the term is used in civil litigation—would be inapplicable. Regardless, as a part of the Federal Government ONC is subject to regulations and policies governing document maintenance and retention, including those promulgated by the National Archives and Records Administration.

Comment: Some commenters expressed interest in more information about documentation and record retention requirements. They wanted to understand how to demonstrate compliance with an information blocking exception.

Response: We did not propose and are not finalizing a record retention requirement specific to the CMP for information blocking. Furthermore, this final rule does not provide additional guidance regarding which documents are required to demonstrate compliance with an ONC exception for information blocking because that is outside the scope of this rule and OIG's authority. OIG will consider any documentation provided by an actor during an investigation to evaluate whether a practice constitutes information blocking.

OIG has 6 years from the date an actor committed a practice that constitutes information blocking to impose a CMP. Section 3022(b)(2)(C) of the PHSA requires that the CMP for information blocking follow the procedures under section 1128A of the SSA, and section 1128A(c)(1) requires that an action for CMPs must be initiated within 6 years from the date the violation occurred.

Even though pursuant to section 1128A of the SSA OIG may commence an action to impose CMPs up to 6 years after the date of a violation, an actor may want to maintain information for additional time beyond 6 years. Actors in a CMP enforcement action bear the burden of proof for affirmative defenses and mitigating circumstances by a preponderance of the evidence. 42 CFR 1005.15(b)(1).

How an actor meets that burden may depend, in part, on records or documentation they maintain. For example, a party may choose to maintain documents demonstrating they meet a specific exception in the information blocking regulations in 45 CFR part 171.

Furthermore, the ONC Final Rule did not establish record retention requirements for actors to maintain documents relating to an exception for a specified period of time. Although ONC did not set record retention duration requirements, ONC explained that many exceptions with documentation conditions are related to other existing regulatory requirements that have document retention standards. For example, the Security Exception at 45 CFR 171.203 is closely aligned to the HIPAA Security Rule, which has a six-year documentation retention requirement in 45 CFR 164.316. 85 FR 25819, May 1, 2020.

We also note that the ONC Final Rule established records and information retention requirements for health IT developers of certified health IT as part of the ONC Health IT Certification Program. The Maintenance of Certification requirement at 45 CFR 170.402(b) generally requires a health IT developer participating in the ONC Health IT Certification Program to retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for a period of 10 years beginning from the date of certification.

2. Effective Date

We proposed two alternative effective dates for the CMP for information blocking. The first proposal proposed an effective date of 60 days from the date of the publication of the final rule. OIG recognized that information blocking is newly regulated conduct and that individuals and entities would require time to take steps to achieve compliance with the ONC Final Rule. The second

proposal proposed that we would set a specific date when OIG's CMP regulations would become effective. OIG specifically proposed an effective date of October 1, 2020, but also noted that we were considering effective dates sooner or later than October 1, 2020. Most of the comments submitted in response to the proposed rule expressed a preference for one of the two proposed approaches. Commenters preferred having a date certain, but no specific effective date was the clear preferred approach by a majority of those who preferred a date certain. Commenters also made several recommendations for alternative approaches.

We are finalizing an effective date for the CMP for information blocking of September 1, 2023.

Comment: Most commenters suggested that OIG adopt a date certain and specifically align the effective date of its CMP for information blocking with the effective dates for the ONC Final Rule and the CMS Interoperability and Patient Access Final Rule (CMS Final Rule) (85 FR 25510, May 1, 2020). Some commenters stated that having a single effective date/enforcement date for all three rules would be beneficial for preparing for compliance with these rules. Some proposed specific, alternative effective dates to allow individuals and entities time to come into compliance. Others did not propose specific effective dates, but proposed an extended period of time between the publication of the final rule and the start of enforcement to permit additional time for ONC to issue additional guidance, for ONC to provide education and outreach, and for OIG to take into consideration the PHE. Some believed that enforcement should begin 3 months after publication of OIG's final rule while several commenters believed the appropriate amount of time was 6 months after publication of this rule. A few commenters suggested that the appropriate amount of time was 1 year or 2 years after publication of this rule. Some commenters supported the proposal for an effective date of the CMP for information blocking to be 60 days after publication of the final rule. The commenters who supported this proposal believed that 60 days after publication provided sufficient time for actors to review and respond to any items that OIG was to outline in its final rule and provide sufficient flexibility and assistance to actors seeking to comply.

Response: Having considered the comments, we are finalizing our proposal for an effective date for the CMP for information blocking at 42 CFR 1003.1400, 1003.1410, and 1003.420 as September 1, 2023. We believe this effective date responds to requests for such a delay. It also addresses commenters' concerns about having time to obtain additional guidance and come into compliance, particularly given the amount of time between the publication of the proposed rule and this final rule. In addition, the selection of this effective date aligns with the goals stated in the proposed rule of providing individuals and entities sufficient time to finalize their ongoing efforts to comply with the ONC information blocking regulations and putting the industry on notice of when penalties will apply to information blocking conduct. This effective date is consistent with the requests of commenters who supported a date certain because those commenters largely sought a specific date to have additional time for compliance efforts. This effective date achieves that goal based on the time between the proposed rule and this rule, which is longer than most specific dates proposed by commenters.

As commenters shared with us in responses to the proposed rule, the PHE has significantly affected the United States, patients, health care providers, and the many individuals and entities that support health care operations. Actors that could be subject to the CMP for information blocking have been responding to COVID–19 on many fronts including addressing information technology-related requirements related to COVID–19, such as reporting data to multiple government agencies. All of this has increased demands on health IT developers of certified health IT, HIEs, and HINs. Recognizing these unprecedented circumstances, the effective date for the CMP for information blocking is reasonable and aligns with the goals stated in the proposed rule. Furthermore, OIG will not impose a CMP on information blocking conduct occurring before the effective date of this final rule.

We reiterate that the effective date of the CMP for information blocking only applies to those actors defined at 45 CFR 171.102 as health IT developers of certified health IT, HINs, and HIEs. We note that the CMP for information blocking does not apply to health care providers except to the extent such health care providers meet the definition of a health IT developer of certified health IT or an HIN/HIE. We discuss in section IV.A.3 of the preamble of this final rule how we evaluate whether health care providers may meet the health IT developer of certified health IT or an HIN/HIE.

3. Basis for Civil Money Penalties for Information Blocking

OIG proposed a basis for the CMP for information blocking at 42 CFR 1003.1400. In setting forth the basis for the CMP in the proposed rule, we proposed that we may impose a CMP against any individual or entity as defined in 45 CFR 171.103(b) that commits information blocking, as defined in 45 CFR part 171. We also proposed that OIG's enforcement would rely on the regulatory definitions set forth by ONC in the ONC Final Rule. Commenters agreed with OIG's proposed approach but requested clarification as to how OIG would interpret the definitions set forth in 45 CFR 171.103(a)(2).

We note that since the publication of the proposed rule, ONC has published the ONC interim final rule (IFR) (85 FR 70064, November 4, 2020) that clarified that 45 CFR 171.103(a)(2) refers to health IT developers of certified health IT rather than health information technology developers.

In this final rule, we finalize 42 CFR 1003.1400 as proposed with a technical correction that incorporates 45 CFR 171.103(a)(2) instead of 45 CFR 171.103(b) and a slight language change to reflect our intent.

Comment: One commenter noted that the regulatory text of our proposed § 1003.1400 should have cited 45 CFR 171.103(a)(2) instead of § 171.103(b) when referring to those individuals or entities subject to civil money penalties.

Response: We agree with the commenter that the correct citation is 45 CFR 171.103(a)(2) and are making this technical correction at 42 CFR 1003.1400. Our intent, as expressed in the proposed rule, was to incorporate ONC's definition of ''information blocking,'' which matches the statutory language in section 3022(a)(1) of the PHSA. This final rule corrects the technical citation error in the proposed rule and is not a substantive change.

We further note that we have changed the language ''as defined in'' to ''as set forth in'' consistent with our intent to incorporate ONC's information blocking regulations in 45 CFR part 171. The regulation at 45 CFR part 171 includes general provisions, including definitions, relevant to the information blocking regulations, as well as the ''exceptions'' to the definition of information blocking. We believe this language change from ''as defined in'' to ''as set forth in'' better reflects our intent to incorporate all of ONC's information blocking regulations into the OIG CMP regulations.

Comment: Commenters requested clarification as to whether they meet the definition of HIN/HIE. Some commenters requested clarification on whether they would meet the definition of HIN/HIE under specific facts, such as by using ONC-certified application programming interface (API) technology as a health care provider, or by engaging in specific processes as a health plan. Some commenters requested clarification as to whether certain types of entities met the definition of HIN/HIE, specifically asking whether a public health institution combating COVID–19, clinical data registries, public health agencies, or a health plan would ever be considered an HIN/HIE. Other commenters requested clarification and examples of when a health care provider would meet the definition of HIN/HIE and be subject to CMPs rather than disincentives. Some commenters suggested that a health care provider or payer should never be considered an HIN/HIE for purposes of the final rule.

Response: OIG will use the definitions in ONC regulations at 45 CFR 171.102 and any guidance issued by ONC when evaluating whether an individual or entity meets the definition of HIN/HIE. Such determinations are individualized and highly dependent on the facts and circumstances presented. Because the ONC definition of HIE/HIN is a functional definition that does not specifically include or exclude any particular individuals or entities, OIG cannot establish in this final rule whether specific individuals or entities or categories of individuals or entities would meet the definition of HIN/HIE as some commenters requested. OIG investigations of information blocking will include gathering facts necessary to assess whether a specific individual or entity meets a definition of health IT developer of certified health IT or HIE/HIN. Furthermore, we proposed following the definitions promulgated in the ONC Final Rule, which are now found at 45 CFR 171.102, and which do not exempt specific types of individuals or entities from the definition of an HIN/HIE that could commit information blocking. Accordingly, we decline to exempt specific types of individuals or entities, including providers or payers, in this final rule.

The ONC regulations define an HIN/HIE as an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI: (1) among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) that is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164. 45 CFR 171.102. When determining whether an individual or entity meets the definition of an HIN/HIE, we may consult with ONC.

In making a fact-specific assessment of whether an individual or entity meets the definition of an HIN/HIE in 45 CFR 171.102, we would assess whether the individual or entity determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI among two or more unaffiliated entities (other than the individual or entity that is the subject of the allegation) that are enabled to exchange with each other for a treatment, payment, or health care operations purpose as such terms are defined in 45 CFR 164.501. As stated in the ONC Final Rule, the definition of HIN/HIE in 45 CFR 171.102 does not cover bilateral exchanges in which an intermediary is simply performing a service on behalf of one entity in providing EHI to another entity or multiple entities and no actual exchange is taking place among all entities. 85 FR 25802, May 1, 2020. The ONC Final Rule also states that for the two unaffiliated individuals or entities besides the HIE/HIN to be enabled, the parties must have the ability and the discretion to exchange with each other under the policies, agreements, technology, and/or services. 85 FR 25802, May 1, 2020. Based on the ONC Final Rule and depending on the specific facts and circumstances, public health institutions, clinical data registries, public health agencies, health plans, and health care providers could meet the definition of an HIN/HIE. As part of our assessment of whether a health care provider or other entity is an HIN/HIE that could be subject to CMPs for information blocking, OIG anticipates engaging with the health care provider or other entity to better understand its functions and to offer the provider an opportunity to explain why it is not an HIN/HIE. We note further that should the definitions in 45 CFR part 171 change in the future, we would continue to look to applicable definitions in 45 CFR part 171 when determining whether an individual or entity was an HIN/HIE at the time of the conduct.

Comment: One commenter noted that the definition of HIN/HIE could apply to individuals serving on HIN governance and advisory committees and requested clarification about whether OIG would direct enforcement against an individual serving on an advisory board for an entity that qualifies as an HIN. The commenter noted that HIEs and HINs rely upon their governance and advisory committees and that individuals subject to enforcement may not want to provide their perspectives or participate on these committees.

Response: While we believe it is unlikely that an individual serving on an HIN/HIE governance and advisory committee would be subject to information blocking enforcement, such individuals could be subject to enforcement if, based on the specific facts, they meet the definition of HIN/HIE and have engaged in information blocking with the requisite intent. To provide transparency on how OIG would assess an allegation involving an individual described by the commenter, we provide the following explanation.

Consistent with section 3022(b)(2)(A) of the PHSA, individuals or entities subject to the CMP for information blocking must fall within a definition in 45 CFR 171.102 that describes one of the categories of actors that are subject to the CMP under section 3022(b)(2)(A) (*i.e.,* developers, networks and exchanges). First, we emphasize that to determine whether an individual on an advisory board met the definition of an HIN/HIE, we would assess the specific facts and circumstances in the case. In assessing whether an individual met the definition of HIN/HIE, OIG would consider the advisory board's purpose and authority to determine, control, or have discretion to administer any requirement policy, or agreement. OIG would also consider the individual's role, the individual's authority, and whether the individual determines, controls, or has the discretion to administer any requirement, policy, or agreement as a member of the advisory board. An individual or entity that does not determine, administer, or have discretion to administer a policy, requirement, or agreement would not meet the definition of an HIN/HIE. For example, the mere act of serving on an advisory board would not mean an individual is an HIN/HIE.

Second, to impose CMPs against an individual, OIG would have to demonstrate that the individual committed an act of information blocking, which includes a requisite intent. Assuming the individual on the

advisory board met the definition of an HIN/HIE, OIG would examine whether the individual engaged in a practice that constituted information blocking. We would analyze the specific practice engaged in by the individual to determine CMP liability. This is consistent with section 3022(a)(6) of the PHSA, which states that information blocking with respect to an individual or entity shall not include an act or practice other than an act or practice committed by such individual or entity. Also consistent with the statute and the implementing regulations in 45 CFR 171.103(a)(2), we would determine whether the individual knew or should have known that the practice in which the individual engaged was likely to interfere with the access, exchange, or use of EHI.

OIG maintains discretion in evaluating what claims to investigate and when to impose CMPs. OIG is not required to—and does not expect to be able to—investigate every allegation it receives. Similarly, OIG may decide it is appropriate to impose CMPs on an entity but not on both an entity and an individual for the same conduct.

Comment: One commenter requested guidance on whether a health care provider would ever be viewed as a health IT developer of certified health IT. The commenter specifically asked whether a health care provider that sublicensed certified health IT to an unaffiliated provider could be subject to CMPs.

Response: A health care provider may meet the definition of a health IT developer of certified health IT in § 171.102, depending on the specific facts and circumstances. This regulatory definition excludes from its scope a health care provider that self-develops health IT for its own use. If any other individual or entity, including a health care provider, develops or offers one or more health IT modules certified under the ONC Health IT Certification Program, then they may meet the definition of health IT developer of certified health IT. If an individual or entity meets the definition of health IT developer of certified health IT and engages in conduct constituting information blocking, then that individual or entity could be subject to CMPs.

Regarding the commenter's specific question, section 3022(b)(1)(A) of the PHSA authorizes OIG to investigate claims of information blocking against any ''other entity offering certified health information technology,'' and the definition of a health IT developer of certified health IT at 45 CFR 171.102 includes an individual or entity that ''offers health information technology.'' ONC further clarified in the ONC Final Rule its policy goal to hold all entities that could, as a developer or offeror, engage in information blocking accountable for their practices that are within the definition of information blocking in 45 CFR 171.103. ONC expressly considered comments to exclude from the definition those entities that only offer technology, rather than modify, configure, or develop it, and declined to do so. 85 FR 25798–99, May 1, 2020. OIG would assess whether a provider that sublicenses technology to an unaffiliated entity meets the definition of a health IT developer of certified health IT at 45 CFR 171.102 based on the specific facts and circumstances.

ONC specifically exempted health care providers that self-develop health IT for their own use from the definition of ''health IT developer of certified health IT.'' The ONC Final Rule clarifies that health care providers that self-develop health IT for their own use refers to health care providers that are the primary users of the health IT and are responsible for its certification status. 85 FR 25799, May 1, 2020. The ONC Final Rule states that ONC interprets ''a health care provider that self-develops health IT for its own use'' to mean that a health care provider does not offer the self-developed health IT to other entities on a commercial basis or otherwise. 85 FR 25799, May 1, 2020. The ONC Final Rule clarifies that a self-developer is not an offeror if it issues login credentials to a licensed health care professional in an independent practice that allow the use of a hospital's electronic health records (EHRs) to furnish and document care to patients in the hospital. 85 FR 25799, May 1, 2020. Whether an individual or entity ''offers health information technology'' requires a fact-specific inquiry, and we expect to consult with ONC in determining whether an individual or entity meets this definition.

As part of any investigation, OIG will need to evaluate whether an individual or entity meets the definition of health IT developer of certified health IT or health information exchange or network. If OIG determines this definition is met and conduct meets the definition of information blocking, OIG may impose CMPs.

Comment: One commenter asked whether a parent company could be subject to CMPs for information blocking based on the conduct of a subsidiary.

Response: Whether information blocking on the part of a subsidiary is attributable to the parent entity depends on the specific facts and circumstances.

Specifically, if a subsidiary acts as the agent of the parent, the parent may be subject to CMPs for the act of the subsidiary if the subsidiary commits information blocking within the scope of agency. Section 3022(b)(2)(C) of the PHSA states that the provisions of section 1128A of the SSA shall apply to a CMP for information blocking. Section 1128A(l) of the SSA states that a principal is liable for penalties, assessments, and exclusion for the acts of the principal's agent acting within the scope of agency.

There may be other instances when information blocking by a subsidiary may create CMP liability for the parent. We note that nothing in the statute or ONC Final Rule precludes such liability, and the ONC Final Rule provides that a health IT developer of certified health IT includes not only the entity that is legally responsible for the certification status of the health IT but could also include any subsidiaries or successors, depending on the specific facts and circumstances of a particular case. 85 FR 25800, May 1, 2020. At this time, we do not have sufficient experience or evidence to delineate specific circumstances where a parent might be liable for information blocking by its subsidiary. We would make any determinations based on the specific facts and circumstances presented.

Comment: One commenter believed that EHR vendors may limit the access of third-party vendors to data, data stores, databases, and endpoints that store data that are not part of the United States Core Data for Interoperability (USCDI).[1] Specifically, the commenter was concerned that an EHR vendor may grant a health care provider access to a database and then deny a third-party vendor the same access. The commenter suggested OIG monitor and penalize EHR vendors that restrict access to data not represented in the USCDI.

Response: Whether a practice constitutes information blocking depends on the specific facts and circumstances. First, the practice must involve EHI as defined in ONC's information blocking regulations. On and after October 6, 2022, EHI for purposes of the information blocking definition in 45 CFR 171.103(a) is not limited to the information identified by data elements represented in the USCDI standard adopted in 45 CFR 170.213, and practices that interfere with access,

[1] USCDI is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.

exchange, or use of any information falling within the definition of EHI in 45 CFR 171.102 may constitute information blocking.

However, even after October 6, 2022, the definition of EHI still excludes certain types of data that an actor may have. For example, EHI does not include psychotherapy notes as defined in 45 CFR 164.501. Therefore, the specific facts and circumstances will determine whether the data that is the subject of a claim of information blocking constitutes EHI.

Second, the practice must constitute information blocking and the individual or entity must have had the requisite intent. We will assess whether the practice is likely to interfere with the access, exchange, or use of EHI, and whether the practice was required by law or met one of the information blocking exceptions. For example, in assessing an allegation similar to the commenter's fact pattern, we may assess whether the health IT developer of certified health IT provided the EHI to the health care provider and the third-party vendor using an alternative manner specified by the third-party vendor consistent with the Content & Manner Exception in 45 CFR 171.301.

Comment: One commenter encouraged OIG to impose CMPs for information blocking on health IT developers of certified health IT with transfer of liability provisions in their contracts. The commenter noted that small and mid-size organizational health care providers are often presented with service contracts that have undesirable terms on a ''take it or leave it'' basis because they may have only one health IT developer available or lack the market share (*i.e.,* leverage) necessary to negotiate out of the undesirable terms.

Response: OIG's information blocking regulations establish the basis for imposing CMPs for information blocking, which is whether the conduct constitutes information blocking as defined in 45 CFR 171.103. The ONC Final Rule established that a variety of contractual provisions could interfere with the access, exchange, and use of EHI and thus implicate the information blocking provision. For example, ONC explained that a contract may implicate the information blocking provision if it includes unconscionable terms for the access, exchange, or use of EHI, or licensing of an interoperability element that could include, but is not limited to, agreeing to indemnify the actor for acts beyond standard practice, such as gross negligence on the part of the actor. ONC explained further that such terms may be problematic with regard to information blocking in situations involving unequal bargaining power relating to accessing, exchanging, and using EHI. 85 FR 25812, May 1, 2020. We will consult with ONC as necessary to inform our determinations as to whether specific service contracts, provisions, and related practices that transfer liability implicate the information blocking provision.

Comment: One commenter stated that the CMS Final Rule requires State Medicaid agencies to make claims with a service date on or after January 1, 2016, available to a beneficiary or a beneficiary's personal representative. But the rule did not specify how long these claims had to be made available. The commenter asked whether the purging of those claims would subject State Medicaid agencies to information blocking penalties.

Response: OIG does not intend to use its authority to investigate information blocking under section 3022(b)(1) of the PHSA to investigate compliance under CMS program requirements. If an investigation uncovers conduct that suggests non-compliance with CMS program requirements, OIG may refer such matters to CMS.

4. Definition of Violation

OIG proposed that a violation be defined as a practice, as defined at 45 CFR 171.102, that constitutes information blocking, as defined at 45 CFR part 171. We have finalized the definition of violation as proposed with a slight modification at 42 CFR 1003.1410(a).

Comment: Many commenters expressed support for our proposed definition of ''violation'' and the incorporation of ONC's definition of ''practice.'' Commenters requested that we provide additional clarity and guidance as to the distinction between a single violation and multiple violations. Other commenters stated that we should provide more specific criteria for identifying a single violation as opposed to multiple violations. Some commenters requested additional clarity as to whether a practice involving multiple patient records would constitute multiple violations.

Response: As finalized in this rule, a violation is a practice, as defined in 45 CFR 171.102, that constitutes information blocking, as set forth in 45 CFR part 171. We note that we have changed the language from ''as defined in'' to ''as set forth in,'' consistent with our intent to incorporate all of ONC's regulations. Whether a practice constitutes a violation depends on the specific facts and circumstances. We did not propose, and therefore this rule does not finalize, specific criteria that we would use to identify single or multiple violations because we do not have enough information or experience with information blocking enforcement to allow us to establish a set of criteria that could apply uniformly to all information blocking allegations. As we gain more experience in assessing allegations, conducting information blocking investigations, and imposing CMPs, we may identify patterns or data that allow us to develop guidance with more specific criteria.

In response to commenters' requests, we are providing below hypothetical examples illustrating how we would determine whether information blocking practices constitute single or multiple violations. The examples set out in the proposed rule at 85 FR 22986–87 remain applicable. But, we clarify that the examples provided in the proposed rule should be understood as involving health IT developers of certified health IT, since health IT developers that do not meet the regulatory definition of health IT developers of certified health IT would not be subject to CMPs. We emphasize that the examples in this preamble and in the preamble to the proposed rule are illustrative, fact-dependent, and not exhaustive. We further note that while our examples discuss the use of health information technology certified under the ONC Certification Program, an individual or entity that meets the definition of a health IT developer of certified health IT or HIE/HIN may engage in conduct that constitutes information blocking relating to health IT certified under the ONC Certification Program, health IT not certified under the ONC Certification Program, or a combination of both.

The following hypothetical examples of conduct assume that the facts meet all the elements of the information blocking definition—including the requisite level of statutory intent.

- A health IT developer (D1) connects to an API supplied by health IT developer of certified health IT (D2). D2's API has been certified to 45 CFR 170.315(g)(10) (standardized API for patient and population services) of the ONC Certification Program and is subject to the ONC Condition of Certification requirements at 45 CFR 170.404 (certified API technology). A health care provider using D1's health IT makes a single request to receive EHI for a single patient via D2's certified API technology. D2 denies this request. OIG would consider this a single violation by D2 affecting a single patient. The violation would consist of D2's denial of

the request to exchange EHI to the provider through D2's certified API.

- A health care provider using technology from a health IT developer (D1) makes a single request to receive EHI for 10 patients through the certified API technology of a health IT developer of health IT (D2). D2 takes a single action to prevent the provider from receiving any patients' information via the API. OIG would consider this as a single violation affecting multiple patients. This is a single violation as D2 took a single action to deny all requests from the provider. The number of patients affected by the violation would be considered when determining the amount of the CMP.
- A health care provider using health IT supplied by a health IT developer (D1) makes multiple, separate requests to receive EHI for several patients via certified API technology supplied by a health IT developer of certified health IT (D2). Each request is for EHI for one or more patients. D2 denies each individual request but does not set up the system to deny all requests made by the health care provider through D2's certified API technology. Thus, D2 is taking separate actions to block individual requests. OIG would consider this conduct to consist of multiple violations affecting multiple patient records. Each denial would be considered a separate violation. The number of patients affected by each violation would be considered in determining the amount of the penalty per violation. We note that for purposes of this example, each denial by D2 constitutes a separate act and thus a separate violation. Thus, if the health care provider using D1's health IT made one request for one patient's EHI, a second request for three patients' EHI, and a third request for five patients' EHI, there would be three separate violations but the penalties may vary due to the number of patients affected by each violation. The action or actions taken by D2 in response to the health care provider's requests provide the basis for assessing whether a practice constitutes a single or multiple violations.
- A health care provider using health IT supplied by a health IT developer (D1) makes multiple requests to receive EHI for a single patient via certified API technology supplied by a health IT developer of certified health IT (D2). But D2 has updated its system to deny all requests made by anyone using D1's technology. Thus, none of the requests by the provider using D1's health IT result in the provider receiving any EHI and D2 always denies requests based on the system change. OIG would consider this practice a single violation. The violation in this case is the singular action to update the system to always deny EHI to anyone requesting to receive the EHI via D1 or D1's health IT. The result of this violation is that all of the requests are denied; however, each individual denial does not constitute a violation. The number of patients affected by D2's denial may constitute an aggravating circumstance resulting in an increased penalty.
- A health IT developer of certified health IT enters into a software license agreement with a health care provider that requires that the health care provider pay a fee for the express purpose of permitting the health care provider to export patients' EHI via the capability certified according to 45 CFR 170.315(b)(10) for switching health IT systems. When the health care provider requests the electronic export, the health IT developer of certified health IT charges the health care provider the fee. We note that the Fees Exception in 45 CFR 171.302 excludes fees charged for an export using functionality certified according to 45 CFR 170.315(b)(10) for purposes of switching health IT. OIG would consider this conduct to include two violations. The first violation would be inclusion of the contract provision (fee) that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. The second violation would be charging the health care provider the fee. Charging the fee in this case constitutes a separate action, and therefore a separate violation from the inclusion of the fee in the software license agreement.

We emphasize that information blocking only requires engaging in a practice that is likely to interfere with, prohibit, or materially discourage the access, exchange, or use of EHI. Information blocking does not require that the practice actually interferes with, prohibits, or materially discourages the access, exchange, or use of EHI.

Comment: One commenter expressed concern that the example in the proposed rule concerning the health IT developer vetting a third-party application might cause health IT developers to forgo necessary security and privacy vetting of applications due to fear of potentially committing an information blocking violation.

Response: In the preamble to the proposed rule, we provided an example where a health IT developer requires vetting of third-party applications before the applications can access the health IT developer's product, but the health IT developer denies applications based on the functionality of the application and not for a privacy or security concern. 85 FR 22987. We note that the ONC Final Rule contained a discussion of vetting, and we agree with the commenter that our example in the preamble to the proposed rule at 85 FR 22987 could benefit from additional explanation.

Before clarifying our example, we provide some of the discussion of ''vetting'' from the ONC Final Rule. First, we note that ''vetting'' in this context is intended to mean a determination regarding whether the application posed a security risk to the health IT developer of certified health IT's software. Second, pursuant to the ONC Final Rule, a vetting process applied in a discriminatory or unreasonable manner could implicate the information blocking provision. 85 FR 25814–17, May 1, 2020. Third, the ONC Final Rule states that for certified API technology (*e.g.,* a Health IT Module certified to § 170.315(g)(10), which includes the use of OAuth2 among other security requirements (see, *e.g.,* 85 FR 25741) in addition to its focus on ''read-only''/responses to requests for EHI to be transmitted, there should be few, if any, security concerns about the risks posed by patient-facing apps to the disclosing actor's health IT systems (because the apps would only be permitted to receive EHI at the patient's decision). Thus, for third-party applications chosen by individuals to facilitate their access to their EHI held by actors, there would generally not be a need for ''vetting'' on security grounds and such vetting actions would be an interference. 85 FR 25815, May 1, 2020. Fourth, actors, such as health care providers, have the ability to conduct whatever ''vetting'' they deem necessary of entities (*e.g.,* app developers) that would be their business associates under HIPAA before granting access and use of EHI to the entities. In this regard, covered entities must conduct necessary vetting in order to comply with the HIPAA Security Rule. 85 FR 25815, May 1, 2020.

With this in mind, we clarify the example as follows. A health IT developer of certified health IT requires vetting of third-party applications to determine whether the applications pose a security risk before the applications are permitted to interface or integrate with the health IT developer of certified health IT's product, which contains EHI. The health IT developer of certified health IT does not apply this vetting process to third party applications selected and authorized by a patient or provider to receive EHI from ''certified API technology,'' as defined as 45 CFR 170.404(c). The health IT developer of certified health IT does not

apply this vetting to patients or API Information Sources, as defined at 45 CFR 170.404(c), which are only receiving EHI through a standardized API. And, the health IT developer of certified health IT does not engage the third-party applications as a business associate or business associate subcontractor. The health IT developer of certified health IT uses vetting to deny EHI access to third-party applications that compete with one of the developer's applications. The health IT developer of certified health IT then denies third-party applications solely on the basis that they compete with one of the developer's applications. Each denial based on the competitive nature of the third-party application is considered a separate violation, as it is a separate act or omission.

If an actor, such as a health IT developer of certified health IT, identifies specific security risks posed by a third-party application, the actor may address those risks consistent with the Security Exception at 45 CFR 171.203 to ensure its practices are not considered information blocking.

Comment: One commenter requested that OIG consider compliance with privacy and security standards as an important factor when evaluating what constitutes a violation.

Response: Both section 3022(a)(1)(A) of PHSA and 45 CFR 171.103(a)(1) exempt from the definition of information blocking practices required by law. Therefore, if a practice is required by privacy or security laws, it does not constitute information blocking. 85 FR 25846, May 1, 2020. However, privacy and security standards that are not required by law (such as trade best practices or voluntary industry standards) would not be exempt from the definition of information blocking, unless an exception applies. When investigating an allegation, we may coordinate with other agencies to understand whether the practice was required under applicable privacy and security laws.

Additionally, ONC established separate Privacy and Security Exceptions at 45 CFR 171.202 and 171.203. If a practice meets all conditions of an exception at all relevant times, then the practice would not be considered information blocking. When investigating an allegation, OIG will assess whether a practice meets an exception.

Comment: Several commenters requested that OIG clarify its view on when the enactment of a policy constitutes information blocking. Commenters requested clarity on whether OIG would view the enactment of a policy that constitutes information blocking as a single violation or multiple violations. Some commenters suggested that consistent and repetitive implementation of a policy should be considered a single violation, regardless of the number of times the policy was applied. Another commenter suggested that we should approach violations and penalties as OCR did in its HIPAA Administrative Simplification Enforcement Final Rule, 71 FR 8390, February 16, 2006, specifically that we should consider a pattern or practice of information blocking to be more violations than a single instance emanating from the same conduct or type of conduct.

Response: We will treat the enactment of a policy that is likely to interfere with, prevent, or materially discourage as one violation. But each enforcement of the policy will constitute another, separate violation. If the creation or existence of the policy alone is what determined the number of violations, and not the number of times the policy was enforced, large organizations with many customers or significant market share would be able to enact policies—regardless of whether they have been written or formalized—and engage in nationwide conduct constituting information blocking against multiple individuals or entities knowing that the maximum penalty would be the statutory maximum of $1 million. A practice is defined as an act or omission by an actor. 45 CFR 171.102. Given that our definition of violation incorporates the word ''practice'' and expressly refers to ONC's definition of practice, the number of violations is connected to the number of discrete acts engaged in by the actor and will depend on the specific facts and circumstances.

5. Determinations Regarding the Penalty Amounts

We proposed to add new 42 CFR 1003.1420 that would codify the statutory factors that OIG must consider when imposing CMPs for committing information blocking. Section 3022(b)(2)(A) of the PHSA mandates that in determining the amount of a CMP for information blocking, OIG must consider factors such as the nature and extent of the information blocking and the harm resulting from such information blocking including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted. The proposed regulatory text included these statutory factors. Given the novel nature of information blocking investigations and enforcement, we recognized in the preamble to the proposed rule that we have limited experience to inform the proposal of additional aggravating and mitigating circumstances to adjust the CMP penalties. Thus, we proposed only to implement the statutory factors described above. We also solicited comment on any additional factors that we should consider for the final rule. We received several comments on proposed factors and a number of recommendations to implement other factors.

We are finalizing 42 CFR 1003.1420 as proposed with a modification to the regulatory text at 42 CFR 1003.1420(a), which is the factor for ''nature and extent of the information blocking.'' For this factor, we have added to the regulatory text the specific facts that section 3022(b)(2)(A) of the PHSA directs us to take into account where applicable: the number of patients affected (42 CFR 1003.1420(a)(1)), number of providers affected (42 CFR 1003.1420(a)(2)), and the number of days the information blocking persisted (42 CFR 1003.1420(a)(3)). In the preamble of the proposed rule, we explained our intent was to specifically implement the exact statutory factors in section 3022(b)(2)(A). 85 FR 22987, April 24, 2020.

Comment: Some commenters requested that OIG consider additional aggravating and mitigating factors when determining the penalty amount it will impose. Commenters suggested considering characteristics of the actor, including an actor's size, market share, whether the actor faced systemic barriers to interoperability, whether the actor took corrective action prior to imposition of a penalty, and the actor's compliance, specifically the actor's history of compliance with the information blocking rules, the robustness of an actor's compliance program, and whether the actor made good faith efforts to seek ONC/OIG guidance. Some commenters suggested considering the consequences of the conduct, such as whether the information blocking resulted in patient harm and the severity of that harm, and whether the information blocking impacted another actor's ability to access information (*i.e.,* interfered with a provider's ability to deliver patient care). Some commenters suggested looking at the specific conduct at issue, specifically whether the information blocking involved a single violation or multiple violations, whether an actor had specific intent to engage in information blocking, whether the actor had control and the extent of that control over the EHI, and whether there were contributory practices by others.

Some commenters suggested that OIG consider mitigating factors beyond an actor's control, such as the effects of natural disasters and public health emergencies (such as the PHE caused by the COVID–19 pandemic) on health care delivery and data exchange. Furthermore, commenters also suggested that practices that exacerbate the negative impact of natural disasters and public health emergencies be considered an aggravating factor. Some commenters suggested that OIG should consider adopting factors based on factors used by OCR in assessing HIPAA CMPs. Some commenters recommended that OIG consider instances of an actor self-disclosing information blocking conduct as a mitigating factor.

Response: We thank commenters for the recommendations of additional aggravating and mitigating factors that OIG should consider. We may consider implementing additional, specific factors in the future via notice and comment rulemaking as we gain more experience in enforcing the CMP for information blocking. At this time, however, we are finalizing the statutory factors listed in section 3022(b)(2)(A) of the PHSA as we proposed, with the modification to the proposed factor for ''nature and extent of the information blocking'' described above.

While we are not adopting additional aggravating and mitigating factors specific to information blocking, we observe that the existing, general factors we must consider under the CMPL will apply to the CMP for information blocking and may address many of the commenters' concerns. The PHSA requires that the provisions of section 1128A of the SSA (other than subsection (a) and (b) of such section) apply to a CMP for information blocking in the same manner as such provisions apply to a CMP or proceeding under section 1128A(a) of the Act. Section 1128A(d) of the SSA requires that OIG, when determining the amount or scope of any assessment, penalty or exclusion imposed under subsection (a), take into account ''(1) the nature of claims and the circumstances under which they were presented, (2) the degree of culpability, history of prior offenses, and financial condition of the person presenting the claims, and (3) such other matters as justice may require.'' 42 U.S.C. 1320a–7a(d). These broad general factors apply to the CMP for information blocking set forth in the PHSA as they do under section 1128A(a) of the SSA. They encompass some of the mitigating or aggravating factors recommended by commenters.

The existing regulatory framework for OIG's CMPs requires that we apply the aggravating and mitigating factors in 42 CFR 1003.140 to the CMP for information blocking determinations in a manner consistent with section 1128A.

As we set forth in the OIG Medicare and State Health Care Programs: Fraud and Abuse Revisions to the Office of Inspector General's Civil Monetary Penalty Rules Final Rule (Revisions Rule), we consider the financial condition of an actor after we evaluate the facts and circumstances of conduct and weigh aggravating and mitigating factors to determine an appropriate penalty and assessment amount. 81 FR 88334, December 7, 2016. Once OIG proposes a penalty amount, the individual or entity may request that OIG consider its ability to pay the proposed amount under procedures discussed in the Revisions Rule at 81 FR 88338.

In addition to the general factors in section 1128A, section 3022(b)(2)(A) of the PHSA specifies a non-exhaustive list of factors that we must consider when imposing CMPs for information blocking. In the proposed rule, we proposed incorporating the PHSA's specific information blocking factors into our existing regulations at new § 1003.1420 of title 42. This new section complements the existing section at 42 CFR 1003.140.

We recognize that the statutory factors enumerated in the PHSA may overlap with the general statutory and regulatory factors for all CMPs in section 1128A of the SSA and in 42 CFR 1003.140. For example, we recognize that ''the nature and circumstances of the violation,'' 42 CFR 1003.140(a)(1), is a similar factor to the ''nature and extent of the information blocking'' and that, consequently, there may be a fact pattern that implicates both factors. We would not apply both or ''double count'' these factors when determining the penalty. We would make a holistic consideration of all aggravating factors when determining the amount of any penalty; this approach would take into account the similarity of the factors.

Many of the commenters' suggested factors, such as whether the information blocking resulted in patient harm and the severity of that harm, whether the actor had specific intent to engage in information blocking, and whether there was one violation or multiple violations, are already encapsulated by the general factors in 42 CFR 1003.140 or the specific information blocking factors in 42 CFR 1003.1410 finalized by this rule. We provide the following examples to illustrate how the issues raised by commenters may be considered when we assess penalty amounts using the two sets of factors at 42 CFR 1003.140 or 1003.1420.

For example, to assess the ''nature and circumstances'' in 42 CFR 1003.140 and ''nature and extent'' of the information blocking in 42 CFR 1003.1420, we will consider the factual nature, circumstances, and extent of the information blocking conduct. Depending on the specific facts and circumstances, these factors may include whether the practice actually interfered with the access, exchange, or use of EHI; the number of violations; whether an actor took corrective action; whether an actor faced systemic barriers to interoperability; to what extent the actor had control over the EHI; the actor's size; and the market share.

Similarly, the general factor in 42 CFR 1003.140 relating to degree of culpability would allow us to consider the commenters' suggested factors relating to whether an actor had actual knowledge or whether an actor had specific intent to engage in information blocking.

Additionally, to assess the ''harm'' factor in 42 CFR 1003.1420, we will consider whether any harm—including physical or financial harm—occurred and evaluate the severity and extent of the harm. In accordance with the statutory language, we will consider the number of patients affected, number of providers affected, and the duration of the information blocking conduct. We recognize that the primary factors set forth at § 1003.140 may also contemplate harm. (For example, in the Revisions Rule, we stated that our consideration of the ''nature and circumstances'' would include ''whether patients were or could have been harmed.'' 81 FR 88337, December 7, 2016.)

With respect to consideration of self-disclosure of information blocking conduct, it is a mitigating circumstance under the general factors at 42 CFR 1003.140(a)(2) for an actor to take appropriate and timely corrective action in response to a violation. Relevant corrective action must include disclosing the violation to OIG through the SDP and fully cooperating with OIG's review and resolution of such disclosure. As discussed in section III.C of the preamble, OIG does not currently have an SDP for information blocking and plans on creating a specific SDP for information blocking after publication of this rule.

We are also not adding factors related to the circumstances surrounding the commission of the act, such as a factor that evaluates whether there were contributory practices by others or an intervening natural disaster. In some

instances, these factors are subsumed in existing general factors. Moreover, section 3022(a)(6) of the PHSA states that ''information blocking, with respect to an individual or entity, shall not include an act or practice other than an act or practice committed by such individual or entity.'' Information blocking, as to health IT developers of certified health IT, HIEs, and HINs, is a practice that an actor ''knows'' or ''should know'' is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI. For example, in the circumstance of an intervening natural disaster that prevents an actor from responding to requests for data, the actor may not have the requisite level of intent. In such a situation, it is unlikely that there would be a sufficient basis to pursue CMPs for information blocking against the actor, and consideration of the factors relating to determination of the amount of any penalty would not be necessary.

Finally, we note that the modification to 42 CFR 1003.1420(a) finalized in this final rule adds three specific facts OIG must consider where applicable (number of patients affected, number of providers, and number of days the information blocking persisted). This modification aligns the factors at § 1003.1420(a) more precisely with the language of the PHSA. As we stated in the proposed rule, section 3022(b)(2)(A) of the PHSA mandates the consideration of the nature and extent of the information blocking and harm resulting from such information blocking including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted. We intended the language of our proposed rule to reflect these statutory factors. 85 FR 22987, April 24, 2020. These factors may also address several of the commenters' concerns related to consideration of impact on patients and providers.

Comment: Some commenters suggested an additional mitigating factor of whether an actor was acting in accordance with another Federal law, State law, or court order limiting or prescribing certain behaviors.

Response: Section 3022(a)(1)(A) of the PHSA and 45 CFR 171.103(a)(1) explicitly exclude conduct that is required by law from the definition of information blocking. Therefore, if an actor's conduct is required by law, it would not meet the definition of information blocking, and OIG would not have the authority to impose CMPs. In the ONC Final Rule, ONC explained that court orders and binding administrative decisions are considered ''required by law.'' 85 FR 25794, May 1, 2020.

Comment: Some commenters sought clarification about how OIG will consider the proposed factors and whether they will be weighted. Some commenters requested additional detail on the range of potential penalty amounts that OIG may issue and the circumstances or thresholds that trigger such penalty amounts. For example, one commenter requested a chart to show how different facts and circumstances would result in different penalty amounts. This commenter also proposed that OIG set a baseline penalty amount to provide guidance on how OIG would set penalties for specific conduct. Some commenters requested clarification on the circumstances and thresholds leading up to the maximum penalty of $1 million. One commenter asked whether penalties assessed would be per organization impacted by the information blocking or per patient impacted by the information blocking.

Response: Our goal in setting penalty amounts is for a penalty to be fair, reasonable, and commensurate with the conduct so that wrongdoers are held accountable and future information blocking conduct is deterred. Accordingly, setting penalty amounts necessitates consideration of the particular facts of each case and does not lend itself to one-size-fits-all formulas or thresholds. The amount of each penalty will be determined per violation and will be based on the aggravating and mitigating factors.

Section 3022(b)(2)(A) of the PHSA requires the consideration of the number of providers affected and the number of patients affected when evaluating the nature and extent of the information blocking and the harm resulting from such information blocking. We consider the number of providers affected and number of patients affected under 42 CFR 1003.1420. In evaluating the nature and extent of the violation, we may also consider the number of organizations impacted by the information blocking, in addition to the number of patients and providers affected.[2]

The penalty amount will be based on a case-specific application of each identified aggravating and mitigating factor. Because penalty amounts require case-by-case evaluation, we decline to set a baseline penalty amount, set thresholds, or create a chart as commenters requested. Similarly, in assessing a penalty amount, OIG may weigh the aggravating and mitigating factors at 42 CFR 1003.140 and 1003.1420, but this weighting will not follow a formula. Application of the aggravating and mitigating factors will result in the penalty assessed being fair and reasonable. We would expect that the maximum penalty of $1 million per violation would apply to particularly egregious conduct.

Comment: Some commenters had concerns that when considering the number of patients and number of providers affected, OIG would impose lower penalty amounts for information blocking against smaller entities, thereby incentivizing information blocking against smaller entities. Other commenters raised concerns that the inclusion and implementation of the ''number of days'' factor in determining CMP amounts would result in an improperly low penalty amount for conduct that had serious effects but did not last long.

Response: Section 3022(b)(2)(A) of the PHSA requires OIG to consider, among other factors, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted. As noted above, OIG's determination of a penalty amount will not rely on a rigid formula for weighing those factors but rather on a case-specific analysis of each identified aggravating and mitigating factor. Nothing in these factors would require OIG to impose a lower CMP amount for information blocking against small entities, even when such entities have fewer patients and providers than larger entities. OIG is mindful that information blocking against small entities can have significant adverse impacts for the entities and their patients and providers. For example, application of the factors at 42 CFR 1003.1420(a) and (b) to the specific facts and circumstances could result in a higher penalty because the information blocking had significant, negative impacts even for short periods of time on an individual or small entities. Moreover, if conduct results in significant harm, including lasting harm to patients, OIG would consider such harm as a potential aggravating factor when determining the appropriate penalty amount.

Comment: Some commenters requested clarification about what OIG considers to be ''harm resulting from'' information blocking. Some commenters suggested OIG should interpret ''harm'' to mean physical harm to a patient's

[2] We could consider the number of organizations under the ''nature and circumstances of the violation'' factor at 42 CFR 1003.140 or the ''nature and extent of information blocking'' at 42 CFR 1003.1420. As we discuss elsewhere in this section IV.A.5 of the preamble, the factors set forth at 42 CFR 1003.140 may overlap at 42 CFR 1003.1420, but we would not double count them.

health and well-being and suggested that OIG also consider financial harm that patients, providers, or third-party actors suffer as a result of information blocking. Other commenters raised concerns that intentional information blockers will be allowed to get away with ''near misses'' if OIG does not consider both the potential and actual harm resulting from information blocking as aggravating factors.

Response: In the proposed rule, we stated that section 3022(b)(2)(A) of the PHSA mandates that OIG must take into consideration factors such as the nature and extent of the information blocking and the harm resulting from such information blocking including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted in determining the amount of a CMP. 85 FR 22987, April 24, 2020. We proposed incorporating these factors at 42 CFR 1003.1420, and noted that these factors were like factors found in other sections of part 1003. We did not propose a definition of ''harm'' in the proposed rule. We solicited comment on this factor and other potential factors we should consider.

In response to commenters' suggestions regarding the types of harm covered by § 1003.1420(b), we agree that ''harm'' should cover both physical and financial harm. Nothing in section 3022(b)(2)(B) of the PHSA indicates that harm should be limited to only one type or a specific type of harm. We are not finalizing a definition of the word harm. We intend to interpret harm in accordance with its plain meaning, ensuring that we can consider a range of harms that may result from information blocking conduct. As we gain more experience investigating and imposing CMPs for information blocking, we may add additional factors related to specific types of harm through rulemaking.

We appreciate the concern regarding intentional information blockers that might get away with ''near misses.'' We do not believe this would be the case. The definition of information blocking applies to conduct that is ''likely'' to interfere with the access, exchange, or use of EHI, thus capturing conduct with a potential to cause harm. With respect to determination of a penalty amount after information blocking is established, as noted above OIG will consider a range of aggravating factors and would not consider ''resulting in harm'' in isolation.

6. Additional Comments

Comment: One commenter noted that the proposed rule stated investigated parties may incur some costs in response to an OIG investigation or enforcement action and encouraged OIG not to impose CMPs unless OIG determined the party committed information blocking. The commenter also asked how investigative fees are calculated in the instance that investigated parties incur costs in response to an OIG investigation or enforcement action.

Response: OIG will impose CMPs where appropriate and does not separately charge costs to investigated parties as the comment contemplates. OIG also does not reimburse investigated parties for costs. We included estimated costs for investigated parties or subjects in the proposed rule as part of our Regulatory Impact Analysis (RIA). The costs described in the RIA only estimate the potential economic impact of the proposed rule, which includes costs that a subject being investigated may incur. For example, a party may incur costs in preparing documents in response to a subpoena or hiring an attorney to represent them during an investigation.

B. CMPs, Assessments, and Exclusions for Fraud or False Claims or Similar Conduct Related to Grants, Contracts, and Other Agreements

The Cures Act amendments to the CMPL authorize the Secretary to impose penalties, assessments, and exclusions for a variety of fraudulent and other improper conduct related to HHS grants, contracts, and other agreements. 42 U.S.C. 1320a–7a(o)–(s). In the proposed rule, we proposed to incorporate this authority into 42 CFR parts 1003 and 1005, which is the existing regulatory framework for the imposition and appeal of OIG penalties, assessments, and exclusions. We received comments related to this authority on only three topics: (1) the proposed definition of ''other agreement'' in 42 CFR 1003.110; (2) the proposed aggravating and mitigating factors in 42 CFR 1003.720 that will be used by OIG to determine the severity of the penalties, assessments, and exclusions it imposes; and (3) OIG enforcement priorities. We received no comments on the definitions we proposed to add to 42 CFR 1003.110 except ''other agreement'' as noted above, and are finalizing those definitions accordingly. We received no comments on 42 CFR 1003.710, which identifies the maximum penalties and assessments OIG may impose for fraud and other improper conduct involving HHS grants, contracts, and other agreements. We also received no comments on changes to 42 CFR 1003.130, 1003.1550, and 1003.1580, which relate to the calculation and collection of assessments imposed under this part and the use of statistical sampling. We finalize 42 CFR 1003.130, 1003.710, 1003.1550, and 1003.1580 as proposed without modification accordingly. We received no comments on 42 CFR 1003.700, which sets forth the bases for OIG's imposition of sanctions for fraud and other improper conduct related to grants, contracts, and other agreements, but are modifying 42 CFR 1003.700(a)(5) for clarity by adding a citation to the existing regulatory definition of ''failure to grant timely access'' at 42 CFR 1003.200(b)(10). We proposed, and are finalizing, that the changes to 42 CFR 1003.110, 1003.130, 1003.700, 1003.710, 1003.720, 1003.1550, and 1003.1580 will be effective 30 days from the publication date of the final rule.

1. Definition of ''Other Agreement''

In the proposed rule, we proposed adopting at 42 CFR 1003.110 the statutory definition of ''other agreement'' that would apply to CMPs brought under 42 CFR 1003.700. This definition includes but is not limited to a cooperative agreement, scholarship, fellowship, loan, subsidy, payment for a specified use, donation agreement, award, or subaward (regardless of whether one or more of the persons entering into the agreement is a contractor or subcontractor). 42 U.S.C. 1320a–7a(q)(3). We noted in the proposed rule that this definition is broad and identifies a nonexclusive list of arrangements that could constitute ''other agreements'' under the statute. We stated that when OIG investigates potential misconduct and decides whether to impose sanctions, it will evaluate matters on a case-by-case basis to determine whether the funding arrangement at issue constitutes an ''other agreement'' under the statute and whether the conduct at issue violates the statute. We are finalizing the definition of ''other agreement'' as proposed in 42 CFR 1003.110, without modification.

Comment: Several commenters requested that OIG provide more detail on which arrangements could constitute ''other agreements'' under the regulation. For example, one commenter asked OIG to provide additional clarity on how OIG will determine which ''other agreements'' fall within the meaning of the statute. Another commenter asked OIG to provide specific examples of scenarios involving ''other agreements'' where it would apply its CMPL authority.

Response: The statutory definition of ''other agreement,'' which has been

incorporated verbatim into 42 CFR 1003.110, is broad and defines ''other agreement'' to include (but not be limited to) a ''cooperative agreement, scholarship, fellowship, loan, subsidy, payment for a specified use, donation agreement, award, or subaward (regardless of whether one or more of the persons entering into the agreement is a contractor or subcontractor).'' It is not possible to identify with specificity all the various types of agreements that may fall under the definition of ''other agreement.'' The nine examples of ''other agreement'' identified in the statute along with the text of 42 U.S.C. 1320a–7a(o)–(s) demonstrate that Congress intended ''other agreement'' to be read broadly to include, for example, not only those direct agreements between the Secretary and recipients of HHS funding but also agreements between recipients of HHS funding and subrecipients such as subcontractors and subawardees. The definition of ''specified claim,'' for example, includes those requests for payment submitted by a subawardee to an HHS awardee that is receiving funding directly from the Secretary. 42 U.S.C. 1320a–7a(r). In addition, 42 U.S.C. 1320a–7a(o)(2) permits OIG to impose sanctions upon an entity that, among other things, creates false documents that are required to be submitted in order to indirectly receive funds from the Secretary. Any person that receives HHS funding directly or indirectly through an agreement is potentially subject to liability under the CMPL if they engage in any of the improper conduct identified in the regulation including but not limited to making misrepresentations in applications for the funding, presenting false or fraudulent specified claims related to the funding, and creating false records related to the funding.

2. Factors in Mitigation and Aggravation

The regulation at 42 CFR 1003.720 of the proposed rule proposed factors for OIG to consider in mitigation and aggravation when determining the appropriate penalty, assessment, and period of exclusion to impose upon persons who engage in fraud and other improper conduct related to HHS grants, contracts, and other agreements. In 42 CFR 1003.720(a), for example, we proposed that OIG would consider identifying as a mitigating factor a circumstance in which the amount of funds involved with the improper conduct was less than $5,000. Then, in 42 CFR 1003.720(b), we proposed considering as an aggravating factor a circumstance in which the amount of funds involved was more than $50,000. We are finalizing 42 CFR 1003.720 as proposed without modification.

Comment: One commenter suggested that the proposed monetary thresholds created in 42 CFR 1003.720(a) and (b) of $5,000 and $50,000 are too low and need to be adjusted upwards because they will lead to overly harsh determinations for CMPL violations related to grants, contracts, and other agreements that involve what the commenter characterized as small amounts of HHS funding. The commenter suggested that OIG consider it a mitigating factor in 42 CFR 1003.720(a) if the amount of funds involved with the improper conduct was less than $50,000 and consider it an aggravating factor in 42 CFR 1003.720(b) if the amount of funds involved with the improper conduct was more than $250,000.

Response: We are not accepting the commenter's suggestion to upwardly adjust the monetary thresholds proposed in 42 CFR 1003.720(a) and (b). The thresholds proposed in 42 CFR 1003.720(a) and (b) are the same thresholds that exist under 42 CFR 1003.220 related to damages sustained by HHS for fraud and similar conduct related to the Federal health care programs. OIG believes it is important for 42 CFR 1003.720 and 1003.220 to be consistent because both provide guidelines for OIG to evaluate the same factor and relate to damages sustained by HHS programs as a result of fraud or similar conduct.

Comment: Two commenters requested that OIG consider as a mitigating circumstance in an action for failure to grant timely access to OIG under 42 CFR 1003.700(a)(5) whether a party acted in good faith in attempting to comply with OIG's request for timely access in matters involving HHS grants, contracts, or other agreements. The commenters both pointed to challenges surrounding the current COVID–19 pandemic as an example of a circumstance in which a party might act in good faith in attempting to comply with OIG's request for access but might be unable to comply with it.

Response: We are not adopting this suggestion. Existing mitigating factors in 42 CFR 1003.140 that apply to all CMPs in 42 CFR part 1003 address commenters' request to assess whether the party acted in good faith as a mitigating factor. As finalized, section 1003.720 identifies factors in mitigation that OIG should consider when imposing sanctions and states that those factors should be read in conjunction with the factors listed in 42 CFR 1003.140. Section 1003.140 requires OIG to consider in mitigation ''the degree of culpability'' of the person against whom a sanction is imposed (42 CFR 1003.140(a)(2)), ''the nature and circumstances of the violation'' (42 CFR 1003.140(a)(1)), and ''such other matters as justice may require'' (42 CFR 1003.140(a)(5)). Under these existing mitigating factors, we would account for a party's good faith in attempting to comply with an OIG timely access request consistent with 42 CFR 1003.140(a)(1), (2), and (5). Therefore, it is unnecessary to explicitly add good faith as a mitigating factor to 42 CFR 1003.720.

3. OIG Enforcement Regarding Grants, Contracts, and Other Agreements

The regulation at 42 CFR 1003.700 identifies the grounds for OIG's imposition of penalties, assessments, and exclusions for fraud and other improper conduct related to HHS grants, contracts, and other agreements, and sets forth the levels of intent required to violate each offense. One commenter asked that OIG only exercise its discretion to impose sanctions when it finds bad intent or other truly abusive, egregious, and intentional wrongdoing. We are not adopting this suggestion and are finalizing 42 CFR 1003.700 as proposed with modification only to 42 CFR 1003.700(a)(5) as discussed below.

Comment: One commenter noted that many HHS grants, contracts, and other agreements are complex and require specific and detailed information from and actions by parties applying for the funds. The commenter also noted that regulatory requirements sometimes change, especially in times of a PHE such as the PHE for COVID–19, and that complying with shifting requirements can be difficult. The commenter asked that OIG take into consideration these complexities, ambiguities, and shifting requirements when exercising its discretion in enforcing the CMPs and that it do so only when the facts demonstrate bad intent or other truly abusive, egregious, and intentional wrongdoing by the parties applying for or receiving HHS funds.

Response: The CMPL authorizes the imposition of penalties, assessments, and exclusions for a variety of fraudulent and other improper conduct related to HHS grants, contracts, and other agreements, and sets forth the levels of intent required to violate each of the offenses it creates. 42 U.S.C. 1320a–7a(o). In determining whether to impose sanctions and the severity of those sanctions, OIG will consider all of the relevant facts and circumstances surrounding an allegation of wrongdoing in light of the factors identified in the CMPL (42 U.S.C.

1320a–7a(d)) and the regulation. 42 CFR 1003.140 and 1003.720. Depending on the facts and circumstances of any particular case, it may be appropriate for OIG to consider the difficulties raised by the commenter, including those related to the PHE for COVID–19, in determining whether a person has violated the CMPL and, if so, the severity of the sanction OIG proposes to impose.

4. Modification to 42 CFR 1003.700(a)(5)

The regulation at 42 CFR 1003.700(a)(5) incorporates into part 1003 OIG's statutory authority under 42 U.S.C. 1320a–7a(o)(5) to impose CMPs, assessments, and exclusions for the failure to grant timely access to OIG for the purpose of audits, investigations, evaluations, or other statutory functions of OIG in matters involving grants, contracts, or other agreements. We stated in the proposed rule at 85 FR 22982 that 42 U.S.C. 1320a–7a(o)(5) largely mirrors the statutory language that has for many years given OIG the authority to impose sanctions for the failure to grant timely access to OIG related to health care claims. Furthermore, we stated at 85 FR 22980 of the proposed rule that it was our intent to incorporate into OIG's existing CMP regulations the new CMP authorities related to fraud and other misconduct involving HHS grants, contracts, and other agreements. However, our proposed regulatory text at 42 CFR 1003.700(a)(5) omitted a citation to the existing regulatory definition of ''failure to grant timely access'' that is located at § 1003.200(b)(10), in a section of part 1003 that relates to fraud involving Federal health care claims. Consistent with our intent to incorporate into part 1003 our authority to impose sanctions for failure to grant timely access related to grants, contracts, and other agreements, our view that this authority mirrors the authority OIG has had for many years related to health care claims and, for clarity, we are finalizing 42 CFR 1003.700(a)(5) with a cross-reference to the existing definition of ''failure to grant timely access'' to make clear that the definition of that term at 42 CFR 1003.200(b)(10) is applicable to actions under 42 CFR 1003.700(a)(5).

C. The Bipartisan Budget Act of 2018

The BBA of 2018 amended the CMPL to increase certain CMP amounts contained in 42 U.S.C. 1320a–7a(a) and (b). The BBA 2018 increased maximum civil money penalties in section 1128A(a) of the SSA (42 U.S.C. 1320a–7a) from $10,000 to $20,000; from $15,000 to $30,000; and from $50,000 to $100,000. The BBA 2018 increased maximum civil money penalties in section 1128A(b) of the SSA from $2,000 to $5,000 in paragraph (1), from $2,000 to $5,000 in paragraph (2), and from $5,000 to $10,000 in paragraph (3)(A)(i). This statutory increase in CMP amounts is effective for acts committed after the date of enactment, February 9, 2018. In the proposed rule, we proposed increasing the civil money penalties in accordance with the BBA 2018. Specifically, for conformity with the CMPL as amended by the BBA 2018, we proposed to revise the civil money penalties contained at 42 CFR 1003.210, 1003.310, and 1003.1010.

The BBA 2018 increased penalty maximums for conduct that occurred after February 9, 2018. Accordingly, for each of the provisions below, we proposed language increasing the maximum penalty for conduct that occurred after February 9, 2018, and maintaining the pre-BBA 2018 penalty maximums for conduct that occurred on or before that date. The penalty amounts for conduct that occurred after February 9, 2018, in proposed 42 CFR 1003.210 were as follows: $20,000 for paragraphs (a)(1), (3), (4), and (8); $30,000 for paragraphs (a)(2) and (9); $100,000 for paragraphs (a)(6) and (7); and $10,000 for paragraph (a)(10)(i). Similarly, we proposed to increase the penalty maximum for conduct that occurred after February 9, 2018, at 42 CFR 1003.310(a)(3) to $100,000, and at 42 CFR 1003.1010(a) to $20,000. We received no comments on this proposal and we are finalizing the penalty amounts as proposed without modification, effective August 2, 2023 as required by the Administrative Procedure Act (APA).

E. Additional Changes to Part 1003

We proposed to change the cross-reference in 42 1003.140(c)(3) to correct a scrivener's error from a prior rulemaking on December 7, 2018. 81 FR 88354. We proposed to add a new paragraph (d)(5) to 42 CFR 1003.140 stating that the penalty amounts in part 1003 are adjusted annually for inflation and eliminating the footnotes 1 through 12 in part 1003 to simplify those sections. We received no comments on these proposed changes, and we are finalizing them with a correction to a typographical error in the regulatory text in the citation to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101–410) effective August 2, 2023.

F. Changes to 42 CFR Part 1005

The procedures set forth in part 1005 govern the appeal of CMPs, assessments, and exclusions in all cases for which OIG has been delegated authority to impose those sanctions including cases involving grants, contracts, and other agreements, and information blocking. As such, we proposed deleting the phrase ''under Medicare or the State health care programs'' from the definitions of ''civil money penalty cases'' and ''exclusion cases'' at 42 CFR 1005.1 to correctly define those terms as applying to all cases for which OIG has been delegated authority to apply CMPs, assessments, and exclusions not only to those cases involving Medicare or the State health care programs. We received no comments regarding this change and are finalizing it as proposed, without modification, in 42 CFR 1005.1, effective August 2, 2023.

IV. Regulatory Impact Statement

We have examined the impact of this final rule as required by Executive Order 12866, the Regulatory Flexibility Act (RFA) of 1980, the Unfunded Mandates Reform Act of 1995, and Executive Order 13132.

A. Executive Order No. 12866

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulations are necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, and public health and safety effects; distributive impacts; and equity). A regulatory impact analysis must be prepared for major rules with significant effects per section 3(f)(1) of Executive Order 12866 (*i.e.,* $200 million or more in any given year). This is not a major rule as defined at 5 U.S.C. 804(2); it is not significant per section 3(f)(1) because it does not reach that economic threshold. The vast majority of Federal health care programs would be minimally impacted from an economic perspective, if at all, by these proposals.

This final rule would enact new statutory enforcement provisions, including new CMP authorities. The regulatory changes implement provisions of the Cures Act and BBA 2018 into 42 CFR parts 1003 and 1005. We believe that the likely aggregate economic effect of these regulations would be significantly less than $100 million.

The expected benefits of the regulation are deterring conduct that negatively affects the integrity of HHS grants, contracts, and other agreements and potentially enhanced statutory compliance by HHS grantees, contractors, and other parties. It also will deter information blocking conduct

that interferes with effective health information exchange and negatively impacts many important aspects of health and health care. We refer readers to the impact analysis of the benefits of prohibiting and deterring information blocking in section XII.C.2.a.(4.2) of the ONC Final Rule, 85 FR 25906, May 1, 2020.

We anticipate that OIG will incur some costs associated with investigation and enforcement of the statutes underlying these penalty provisions. The Consolidated Appropriations Act, 2022 appropriates to OIG funding necessary for carrying out information blocking activities. Public Law 117–103, March 15, 2022. Additionally, investigated parties may incur some costs in response to an OIG investigation or enforcement action. Absent information about the frequency of prohibited conduct, we are unable to determine precisely the potential costs of this regulation.

Civil money penalties and assessments, if any, would be considered transfers. However, we are unable to reliably estimate potential penalty and assessment amounts because enforcement action will depend on the facts and circumstances of individual cases, some conduct subject to enforcement will be newly regulated, and some cases may result in settlement. We did not receive any comments on potential impacts of the rulemaking.

B. Regulatory Flexibility Act

The RFA and the Small Business Regulatory Enforcement and Fairness Act of 1996, which amended the RFA, require agencies to analyze options for regulatory relief of small businesses. For purposes of the RFA, small entities include small businesses, nonprofit organizations, and Government agencies.

The Department considers a rule to have a significant impact on a substantial number of small entities if it has an impact of more than 3 percent of revenue for more than 5 percent of affected small entities. This final rule should not have a significant impact on the operations of a substantial number of small entities, as these changes would not impose any new requirement on any party. These changes largely enact existing regulatory authority. In addition, we expect that increases in the maximum penalty finalized here will only have an impact in a small number of cases. As a result, we have concluded that this final rule likely will not have a significant impact on a substantial number of small entities and that a regulatory flexibility analysis is not required for this rulemaking.

In addition, section 1102(b) of the SSA (42 U.S.C. 1302) requires us to prepare a regulatory impact analysis if a rule under Titles XVIII or XIX or section B of Title XI of the SSA may have a significant impact on the operations of a substantial number of small rural hospitals. We have concluded that this final rule should not have a significant impact on the operations of a substantial number of small rural hospitals because these changes would not impose any requirement on any party and small rural hospitals are not subject to CMPs for information blocking under this final rule. Therefore, a regulatory impact analysis under section 1102(b) is not required for this rulemaking.

C. Unfunded Mandates Reform Act

Section 202 of the Unfunded Mandates Reform Act of 1995, Public Law 104–4, also requires that agencies assess anticipated costs and benefits before issuing any rule that may result in expenditures in any one year by State, local, or Tribal governments in the aggregate, or by the private sector, of $100 million, adjusted annually for inflation. We believe that there are no significant costs associated with these revisions that would impose any mandates on State, local, or Tribal governments or the private sector that would result in an expenditure of $158 million (after adjustment for inflation) or more in any given year and that a full analysis under the Unfunded Mandates Reform Act is not necessary.

D. Executive Order 13132

Executive Order 13132, Federalism, establishes certain requirements that an agency must meet when it promulgates a rule that imposes substantial direct requirements or costs on State and local governments, preempts State law, or otherwise has federalism implications. In reviewing this rule under the threshold criteria of Executive Order 13132, we have determined that this final rule would not significantly affect the rights, roles, and responsibilities of State or local governments. Nothing in this final rule imposes substantial direct requirements or 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 provisions in this final rule.

The Secretary is authorized by 42 U.S.C. 1320a–7a(o), which we enact in the regulation at 42 CFR 1003.700, to impose CMPs and assessments against individuals and entities that engage in fraud and other improper conduct against specified State agencies that administer or supervise the administration of grants, contracts, and other agreements funded in whole or in part by the Secretary. Additionally, 42 U.S.C. 1320a–7a(f)(4) directs that these CMPs and assessments be deposited into the Treasury of the United States. Amounts collected under this authority could not be used to compensate a State for damages it incurs due to improper conduct related to grants, contracts, or other agreements funded by the Secretary that are administered or supervised by specified State agencies.

However, neither 42 U.S.C. 1320a–7a nor this final rule preclude or impede any State's authority to pursue actions against entities and individuals that defraud or otherwise engage in improper conduct related to grants, contracts, or other agreements funded by the Secretary that are administered or supervised by specified State agencies. For this reason, the Secretary's authority related to specified State agencies will not have a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

Based on OIG's prior approach to enforcement that involves State programs and agencies, we also anticipate coordinating closely with the relevant State authorities, which would provide States notice about the improper conduct and the opportunity to pursue action under the State authority.

V. Paperwork Reduction Act

These changes to parts 1003 and 1005 impose no new reporting requirements or collections of information. Therefore, a Paperwork Reduction Act review is not required.

List of Subjects

42 CFR Part 1003

Contracts, Fraud, Grant programs—health, Information blocking, Penalties.

42 CFR Part 1005

Administrative practice and procedure.

For the reasons stated in the preamble, the Office of Inspector General, Department of Health and Human Services, amends 42 CFR chapter V, subchapter B, as follows:

PART 1003—CIVIL MONEY PENALTIES, ASSESSMENTS AND EXCLUSIONS

■ 1. Revise the authority citation for part 1003 to read as follows:

Authority: 42 U.S.C. 262a, 300jj–52, 1302, 1320a–7, 1320a–7a, 1320b–10, 1395u(j), 1395u(k), 1395cc(j), 1395w–141(i)(3), 1395dd(d)(1), 1395mm, 1395nn(g), 1395ss(d), 1396b(m), 11131(c), and 11137(b)(2).

■ 2. Amend § 1003.100 by:
■ a. Revising paragraph (a); and
■ b. In paragraph (b)(1), adding ''(CMPs)'' following ''civil money penalties'' and a semicolon following ''this part''.

The revision reads as follows:

§ 1003.100 Basis and purpose.

(a) *Basis.* This part implements sections 1128(c), 1128A, 1140, 1819(b)(3)(B), 1819(g)(2)(A), 1857(g)(2)(A), 1860D–12(b)(3)(E), 1860D–31(i)(3), 1862(b)(3)(C), 1867(d)(1), 1876(i)(6), 1877(g), 1882(d), 1891(c)(1); 1903(m)(5), 1919(b)(3)(B), 1919(g)(2)(A), 1927(b)(3)(B), 1927(b)(3)(C), and 1929(i)(3) of the Social Security Act; sections 421(c) and 427(b)(2) of Public Law 99–660; section 201(i) of Public Law 107–188 (42 U.S.C. 1320a–7(c), 1320a–7a, 1320b–10, 1395i–3(b)(3)(B), 1395i–3(g)(2)(A), 1395w–27(g)(2)(A), 1395w–112(b)(3)(E), 1395w–141(i)(3), 1395y(b)(3)(B), 1395dd(d)(1), 1395mm(i)(6), 1395nn(g), 1395ss(d), 1395bbb(c)(1), 1396b(m)(5), 1396r(b)(3)(B), 1396r(g)(2)(A), 1396r–8(b)(3)(B), 1396r–8(b)(3)(C), 1396t(i)(3), 11131(c), 11137(b)(2), and 262a(i)); and section 3022 of the Public Health Service Act (42 U.S.C. 300jj–52).

* * * * *

■ 3. Amend § 1003.110 by:
■ a. Adding the definitions of ''Department,'' ''Obligation,'' ''Other agreement,'' and ''Program beneficiary'' in alphabetical order;
■ b. Revising the definition of ''Reasonable request;'' and
■ c. Adding the definitions of ''Recipient,'' ''Specified claim,'' and ''Specified State agency'' in alphabetical order.

The revision and additions read as follows:

§ 1003.110 Definitions.

* * * * *

Department means the Department of Health and Human Services.

* * * * *

Obligation for the purposes of § 1003.700 means an established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship for a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment.

Other agreement for the purposes of § 1003.700 includes a cooperative agreement, scholarship, fellowship, loan, subsidy, payment for a specified use, donation agreement, award, or subaward (regardless of whether one or more of the persons entering into the agreement is a contractor or subcontractor).

* * * * *

Program beneficiary means—in the case of a grant, contract, or other agreement designed to accomplish the objective of awarding or otherwise furnishing benefits or assistance to individuals and for which the Secretary provides funding—an individual who applies for or who receives such benefits or assistance from such grant, contract, or other agreement. Such term does not include—with respect to such grant, contract, or other agreement—an officer, employee, or agent of a person or entity that receives such grant or that enters into such contract or other agreement.

Reasonable request with respect to §§ 1003.200(b)(10) and 1003.700(a)(5) means a written request signed by a designated representative of the OIG and made by a properly identified agent of the OIG during reasonable business hours. The request will include:

(1) A statement of the authority for the request;

(2) The person's rights in responding to the request;

(3) The definition of ''reasonable request'' and ''failure to grant timely access'' under this part;

(4) The deadline by which the OIG requests access; and

(5) The amount of the civil money penalty or assessment that could be imposed and the effective date, length, and scope and effect of the exclusion that would be imposed for failure to comply with the request, and the earliest date that a request for reinstatement would be considered.

Recipient for the purposes of § 1003.700 means any person (excluding a program beneficiary as defined in this section) directly or indirectly receiving money or property under a grant, contract, or other agreement funded in whole or in part by the Secretary, including a subrecipient or subcontractor.

* * * * *

Specified claim means any application, request, or demand under a grant, contract, or other agreement for money or property, whether or not the United States or a specified State agency has title to the money or property, that is not a claim (as defined in this section) and that:

(1) Is presented or caused to be presented to an officer, employee, or agent of the Department or agency thereof, or of any specified State agency; or

(2) Is made to a contractor, grantee, or other recipient if the money or property is to be spent or used on the Department's behalf or to advance a Department program or interest, and if the Department:

(i) Provides or has provided any portion of the money or property requested or demanded; or

(ii) Will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded.

Specified State agency means an agency of a State government established or designated to administer or supervise the administration of a grant, contract, or other agreement funded in whole or in part by the Secretary.

* * * * *

■ 4. Revise § 1003.130 to read as follows:

§ 1003.130 Assessments.

The assessment in this part is in lieu of damages sustained by the Department, a State agency, or a specified State agency because of the violation.

■ 5. Amend § 1003.140 by:
■ a. In paragraph (c)(3), removing the phrase ''(as defined by paragraph (e)(2) of this section)'' and adding the phrase ''(as defined by paragraph (d)(2) of this section)'' in its place.
■ b. Adding paragraph (d)(5).

The addition reads as follows:

§ 1003.140 Determinations regarding the amount of penalties and assessments and the period of exclusion.

* * * * *

(d) * * *

(5) The penalty amounts in this part are updated annually, as adjusted in accordance with the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (section 701 of Pub. L. 114–74). Annually adjusted amounts are published at 45 CFR part 102.

■ 6. Amend § 1003.210 by revising paragraphs (a)(1) through (4) and (6) through (9), (a)(10) introductory text, and (a)(10)(i) to read as follows:

§ 1003.210 Amount of penalties and assessments.

(a) * * *

(1) Except as provided in this section, the OIG may impose a penalty of not more than $10,000 for conduct that occurred on or before February 9, 2018, and not more than $20,000 for conduct that occurred after February 9, 2018, for each individual violation that is subject to a determination under this subpart.

(2) The OIG may impose a penalty of not more than $15,000 for conduct that occurred on or before February 9, 2018, and not more than $30,000 for conduct that occurred after February 9, 2018, for each person with respect to whom a determination was made that false or misleading information was given under § 1003.200(b)(2).

(3) The OIG may impose a penalty of not more than $10,000 for conduct that occurred on or before February 9, 2018, and not more than $20,000 for conduct that occurred after February 9, 2018, per day for each day that the prohibited relationship described in § 1003.200(b)(3) occurs.

(4) For each individual violation of § 1003.200(b)(4), the OIG may impose a penalty of not more than $10,000 for conduct that occurred on or before February 9, 2018, and not more than $20,000 for conduct that occurred after February 9, 2018, for each separately billable or non-separately-billable item or service provided, furnished, ordered, or prescribed by an excluded individual or entity.

* * * * *

(6) The OIG may impose a penalty of not more than $50,000 for conduct that occurred on or before February 9, 2018, and not more than $100,000 for conduct that occurred after February 9, 2018, for each false statement, omission, or misrepresentation of a material fact in violation of § 1003.200(b)(7).

(7) The OIG may impose a penalty of not more than $50,000 for conduct that occurred on or before February 9, 2018, and not more than $100,000 for conduct that occurred after February 9, 2018, for each false record or statement in violation of § 1003.200(b)(9).

(8) The OIG may impose a penalty of not more than $10,000 for conduct that occurred on or before February 9, 2018, and not more than $20,000 for conduct that occurred after February 9, 2018, for each item or service related to an overpayment that is not reported and returned in accordance with section 1128J(d) of the Act in violation of § 1003.200(b)(8).

(9) The OIG may impose a penalty of not more than $15,000 for conduct that occurred on or before February 9, 2018, and not more than $30,000 for conduct that occurred after February 9, 2018, for each day of failure to grant timely access in violation of § 1003.200(b)(10).

(10) For each false certification in violation of § 1003.200(c), the OIG may impose a penalty of not more than the greater of:

(i) $5,000 for conduct that occurred on or before February 9, 2018, and $10,000 for conduct that occurred after February 9, 2018; or

* * * * *

■ 7. Amend § 1003.310 by revising paragraph (a)(3) to read as follows:

§ 1003.310 Amount of penalties and assessments.

(a) * * *

(3) $50,000 for conduct that occurred on or before February 9, 2018, and $100,000 for conduct that occurred after February 9, 2018, for each offer, payment, solicitation, or receipt of remuneration that is subject to a determination under § 1003.300(d).

* * * * *

■ 8. Add subpart G (consisting of §§ 1003.700, 1003.710, and 1003.720) to read as follows:

Subpart G—CMPs, Assessments, and Exclusions for Fraud or False Claims or Similar Conduct Related to Grants, Contracts, and Other Agreements

Sec.

§ 1003.700 Basis for civil money penalties, assessments, and exclusions.

The OIG may impose a penalty, assessment, and an exclusion against any person including an organization, agency, or other entity, but excluding a program beneficiary (as defined in § 1003.110), that, with respect to a grant, contract, or other agreement for which the Secretary provides funding:

(a) Knowingly presents or causes to be presented a specified claim (as defined in § 1003.110) under such grant, contract, or other agreement that the person knows or should know is false or fraudulent;

(b) Knowingly makes, uses, or causes to be made or used, any false statement, omission, or misrepresentation of a material fact in any application, proposal, bid, progress report, or other document that is required to be submitted in order to directly or indirectly receive or retain funds provided in whole or in part by such Secretary pursuant to such grant, contract, or other agreement;

(c) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent specified claim under such grant, contract, or other agreement;

(d) Knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation (as defined in § 1003.110) to pay or transmit funds or property to such Secretary with respect to such grant, contract, or other agreement, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit funds or property to such Secretary with respect to such grant, contract, or other agreement; or

(e) Fails to grant timely access (as defined in § 1003.200(b)(10)), upon reasonable request (as defined in § 1003.110), to the Inspector General of the Department, for the purpose of audits, investigations, evaluations, or other statutory functions of such Inspector General in matters involving such grants, contracts, or other agreements.

§ 1003.710 Amount of penalties and assessments.

(a) *Penalties.* (1) In cases under § 1003.700(a)(1), the OIG may impose a penalty of not more than $10,000 for each specified claim.

(2) In cases under § 1003.700(a)(2), the OIG may impose a penalty of not more than $50,000 for each false statement, omission, or misrepresentation of a material fact.

(3) In cases under § 1003.700(a)(3), the OIG may impose a penalty of not more than $50,000 for each false record or statement.

(4) In cases under § 1003.700(a)(4), the OIG may impose a penalty of not more than $50,000 for each false record or statement or not more than $10,000 for each day that the person knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay.

(5) In cases under § 1003.700(a)(5), the OIG may impose a penalty of not more than $15,000 for each day of the failure described in § 1003.700(a)(5).

(b) *Assessments.* (1) In cases under § 1003.700(a)(1) and (3), such a person shall be subject to an assessment of not more than three times the amount claimed in the specified claim described in § 1003.700(a)(1) and (3) in lieu of damages sustained by the United States or a specified State agency because of such specified claim.

(2) In cases under § 1003.700(a)(2) and (4), such a person shall be subject to an assessment of not more than three times the total amount of the funds described in § 1003.700(a)(2) and (4), respectively (or, in the case of an obligation to transmit property to the Secretary described in § 1003.700(a)(4), of the

value of the property described in § 1003.700(a)(4)) in lieu of damages sustained by the United States or a specified State agency because of such case.

§ 1003.720 Determinations regarding the amount of penalties and assessments and period of exclusion.

In considering the factors listed in § 1003.140:

(a) It should be considered a mitigating circumstance if all the violations included in the action brought under this part were of the same type and occurred within a short period of time, there were few such violations, and the total amount claimed or requested related to the violations was less than $5,000.

(b) Aggravating circumstances include but are not limited to:

(1) The violations were of several types or occurred over a lengthy period of time;

(2) There were many such violations (or the nature and circumstances indicate a pattern of false or fraudulent specified claims, requests for payment, or a pattern of violations);

(3) The amount requested or claimed or related to the violations was $50,000 or more; or

(4) The violation resulted, or could have resulted, in physical harm to any individual.

§ 1003.1010 [Amended]

■ 9. Amend § 1003.1010 in paragraph (a) by removing the figure ''$10,000'' and adding in its place the phrase ''$10,000 for conduct that occurred on or before February 9, 2018, and $20,000 for conduct that occurred after February 9, 2018,''.

■ 10. Effective September 1, 2023, add subpart N (consisting of §§ 1003.1400, 1003.1410, and 1003.1420) to read as follows:

Subpart N—CMPs for Information Blocking

Sec.

§ 1003.1400 Basis for civil money penalties.

The OIG may impose a civil money penalty against any individual or entity described in 45 CFR 171.103(a)(2) that commits information blocking, as set forth in 45 CFR part 171.

§ 1003.1410 Amount of penalties.

The OIG may impose a penalty of not more than $1,000,000 per violation.

(a) For this subpart, *violation* means a practice, as defined in 45 CFR 171.102, that constitutes information blocking, as set forth in 45 CFR part 171.

(b) [Reserved]

§ 1003.1420 Determinations regarding the amount of penalties.

In considering the factors listed in § 1003.140, the OIG shall take into account:

(a) The nature and extent of the information blocking including where applicable:

(1) The number of patients affected;

(2) The number of providers affected; and

(3) The number of days the information blocking persisted; and

(b) The harm resulting from such information blocking including where applicable:

(1) The number of patients affected;

(2) The number of providers affected; and

(3) The number of days the information blocking persisted.

§ 1003.1550 [Amended]

■ 11. Amend § 1003.1550 in paragraph (b) by removing the phrase ''where the claim'' and adding the phrase ''where the claim or specified claim'' in its place.

■ 12. Amend § 1003.1580 by revising paragraph (a) to read as follows:

§ 1003.1580 Statistical sampling.

(a) In meeting the burden of proof in § 1005.15 of this chapter, the OIG may introduce the results of a statistical sampling study as evidence of the number and amount of claims, specified claims, and/or requests for payment, as described in this part, that were presented, or caused to be presented, by the respondent. Such a statistical sampling study, if based upon an appropriate sampling and computed by valid statistical methods, shall constitute prima facie evidence of the number and amount of claims, specified claims, or requests for payment, as described in this part.

* * * * *

§§ 1003.210, 1003.310, 1003.410, 1003.510, 1003.610, 1003.810, 1003.910, 1003.1010, 1003.110, 1003.1210, and 1003.1310 [Amended]

■ 13. In addition to the amendments set forth above, in 42 CFR part 1003, amend each section referenced in the first column of the following table by removing the footnote referenced in the second column.

Section	Footnote
1003.210(a) heading	1
1003.310(a) heading	2
1003.410(a) heading	3
1003.410(b)(2)	4
1003.510 introductory text	5
1003.610(a) introductory text	6
1003.810 introductory text	7
1003.910	8
1003.1010 introductory text	9
1003.1110 introductory text	10
1003.1210 introductory text	11
1003.1310	12

PART 1005—APPEALS OF EXCLUSIONS, CIVIL MONEY PENALTIES AND ASSESSMENTS

■ 14. The authority citation for part 1005 continues to read as follows:

Authority: 42 U.S.C. 405(a), 405(b), 1302, 1320a–7, 1320a–7a and 1320c–5.

■ 15. Amend § 1005.1 by revising the definitions of ''Civil money penalty cases'' and ''Exclusion cases'' to read as follows:

§ 1005.1 Definitions.

Civil money penalty cases refers to all proceedings arising under any of the statutory bases for which the OIG has been delegated authority to impose civil money penalties (CMPs).

* * * * *

Exclusion cases refers to all proceedings arising under any of the statutory bases for which the OIG has been delegated authority to impose exclusions.

* * * * *

Dated: June 26, 2023.

Xavier Becerra,

Secretary.

[FR Doc. 2023–13851 Filed 6–30–23; 8:45 am]

BILLING CODE 4152–01–P