session and a presentation on Hospital Acquired Conditions (HAC) and POA background. A brief overview regarding the implementation strategy for selecting the hospital-acquired conditions will then be presented. Next, a review of the conditions included in the FY 2008 hospital inpatient prospective payment systems (IPPS) final rule with comment period will be presented followed by a public comment session. There will be a lunch break from approximately 1 to 2 p.m., e.s.t. Following lunch, there will be presentations on the following: (1) The role of providers in documentation; (2) POA Indicator Reporting; and (3) HAC & POA Outreach and Education. An additional public comment period will follow the presentations. The meeting will conclude by 5 p.m., e.s.t.

III. Registration Instructions

For security reasons, any persons wishing to attend this meeting must register by the date listed in the DATES section of this notice. Persons interested in attending the meeting or listening by teleconference must register by completing the on-line registration located at *http://registration.intercall.com/go/cms2.* The on-line registration system will generate a confirmation page to indicate the completion of your registration. Please print this page as your registration receipt.

Individuals may also participate in the listening session by teleconference. Registration is required as the number of call-in lines will be limited. The call-in number will be provided upon confirmation of registration.

An audio download of the listening session will be available through the CMS HAC and POA Indicator Web site at *http://www.cms.hhs.gov/HospitalAcqCond/01_Overview.asp* after the listening session.

IV. Security, Building, and Parking Guidelines

This meeting will be held in a Federal government building; therefore, Federal security measures are applicable. In planning your arrival time, we recommend allowing additional time to clear security. The on-site check-in for visitors will begin at 9 a.m., e.s.t. Please allow sufficient time to complete security checkpoints.

Security measures include the following:

- Presentation of government-issued photographic identification to the Federal Protective Service or Guard Service personnel.
- Interior and exterior inspection of vehicles (this includes engine and trunk inspection) at the entrance to the grounds. Parking permits and instructions will be issued after the vehicle inspection.
- Passing through a metal detector and inspection of items brought into the building. We note that all items brought to CMS, whether personal or for the purpose of demonstration or to support a demonstration, are subject to inspection.

We cannot assume responsibility for coordinating the receipt, transfer, transport, storage, set-up, safety, or timely arrival of any personal belongings or items used for demonstration or to support a demonstration.

Note: Individuals who are not registered in advance will not be permitted to enter the building and will be unable to attend the meeting. The public may not enter the building earlier than 30 to 45 minutes prior to the convening of the meeting.

All visitors must be escorted in areas other than the lower and first floor levels in the Central Building. Seating capacity is limited to the first 550 registrants.

Authority: Section 5001(c) The Deficit Reduction Act (DRA) of 2005.

Dated: November 16, 2007.

Kerry Weems,

Acting Administrator, Centers for Medicare & Medicaid Services.

[FR Doc. 07–5801 Filed 11–21–07; 8:45 am]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of a Modified or Altered System of Records

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS).

ACTION: Notice of a Modified or Altered System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter an SOR, ''Employee Building Pass File (EBP) System, System No. 09–70–3002,'' last published at 67 FR 40937 (June 14, 2002). We propose to assign a new CMS identification number to this system to simplify the obsolete and confusing numbering system originally designed to identify the Bureau, Office, or Center that maintained information in the Health Care Financing Administration systems of records. The new assigned identifying number for this system should read: System No. 09–70–0529.

We propose to modify existing routine use number 2 that permits disclosure to agency contractors and consultants to include disclosure to CMS grantees who perform a task for the agency. CMS grantees, charged with completing projects or activities that require CMS data to carry out that activity, are classified separately from CMS contractors and/or consultants. The modified routine use will remain as routine use number 1. We will delete routine use number 3 authorizing disclosure to support constituent requests made to a congressional representative. If an authorization for the disclosure has been obtained from the data subject, then no routine use is needed. The Privacy Act allows for disclosures with the ''prior written consent'' of the data subject.

Finally, we will delete the section titled ''Additional Circumstances Affecting Routine Use Disclosures,'' that addresses ''Protected Health Information (PHI)'' and ''small cell size.'' The requirement for compliance with HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' does not apply because this system does not collect or maintain PHI. In addition, our policy to prohibit release if there is a possibility that an individual can be identified through ''small cell size'' is not applicable to the data maintained in this system.

We are modifying the language in the remaining routine uses to provide a proper explanation as to the need for the routine use and to provide clarity to CMS's intention to disclose individual-specific information contained in this system. The routine uses will then be prioritized and reordered according to their usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization or because of the impact of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Pub. L. 108–173) provisions and to update language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of the SOR is to issue and control United States Government building passes issued to all CMS employees and non-CMS employees who require continuous access to CMS buildings in Baltimore and other CMS and HHS facilities. Information retrieved from this SOR will be used to: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or grantee; (2) assist other Federal agencies with activities related to this system; and (3) support litigation

involving the Agency. We have provided background information about the modified system in the **SUPPLEMENTARY INFORMATION** section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See *Effective Dates* section for comment period.

DATES: *Effective Dates:* CMS filed a modified system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Homeland Security and Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on November 15, 2007. To ensure that all parties have adequate time in which to comment, the modified SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: CMS Privacy Officer, Division of Privacy Compliance, Enterprise Architecture and Strategy Group, Office of Information Services, CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.–3 p.m., Eastern Time zone.

FOR FURTHER INFORMATION CONTACT: Marcia Levin, Security System Administrator, Emergency Management and Response Group, Office of Operations Management, CMS, Room SLL–11–28, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Ms. Levin can be reached by telephone at 410–786–7840, or via e-mail at *Marcia.Levin@cms.hhs.gov*.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified or Altered System of Records

A. Statutory and Regulatory Basis for SOR

Authority for maintenance of this system of records is given under Section 5 United States Code (U.S.C.) 301, 40 USCA 121(c)(2), and 41 Code of Federal Regulations (CFR) 102–74.375.

B. Collection and Maintenance of Data in the System

The system contains information on Federal employees, contractors, consultants or grantees, Government Services Administration employees, and contract guards working in CMS's central office complex in Baltimore, Maryland, and other CMS and HHS Federal buildings. The system contains the name of the employee or other authorized individuals, social security number, identification card number, building/work location, phone number, position, title, grade, supervisor's name and telephone number.

II. Agency Policies, Procedures, and Restrictions on Routine Uses

A. The Privacy Act permits us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such disclosure of data is known as a ''routine use.'' The government will only release EBP information that can be associated with an individual as provided for under ''Section III. Proposed Routine Use Disclosures of Data in the System. '' Both identifiable and non-identifiable data may be disclosed under a routine use.

We will only disclose the minimum personal data necessary to achieve the purpose of EBP. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure and only after CMS:

1. Determines that the use or disclosure is consistent with the reason data is being collected; e.g., to issue and control United States Government building passes issued to all CMS employees and non-CMS employees who require continuous access to CMS buildings in Baltimore and other CMS and HHS facilities.

2. Determines that:

a. The purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;

b. The purpose for which the disclosure is to be made is of sufficient importance to warrant the effect and/or risk on the privacy of the individual that additional exposure of the record might bring; and

c. There is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

3. Requires the information recipient to:

a. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

b. Remove or destroy at the earliest time all patient-identifiable information; and

c. Agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the EBP without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, consultants, or grantees who have been contracted by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system and who need to have access to the records in order to assist CMS.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing CMS functions relating to purposes for this system.

CMS occasionally contracts out certain of its functions when this would contribute to effective and efficient operations. CMS must be able to give a contractor, consultants, or grantees whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor, consultants, or grantees from using or disclosing the information for any purpose other than that described in the contract and to return or destroy all information at the completion of the contract.

2. To assist other Federal agencies with activities related to this system and who need to have access to the records in order to perform the activity.

The Federal Protection Service may require EBP data to enable them to assist in inquiries about an individual's

authorization to enter CMS's central office complex in Baltimore, Maryland and other CMS and HHS Federal buildings.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with another Federal agency to assist in accomplishing CMS functions relating to purposes for this SOR.

3. To the Department of Justice (DOJ), court or adjudicatory body when

a. the Agency or any component thereof; or

b. any employee of the Agency in his or her official capacity; or

c. any employee of the Agency in his or her individual capacity where the DOJ has agreed to represent the employee; or

d. the United States Government;

is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court or adjudicatory body involved. A determination would be made in each instance that, under the circumstances involved, the purposes served by the use of the information in the particular litigation is compatible with a purpose for which CMS collects the information.

IV. Safeguards

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations include but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications; HHS Information Systems Program Handbook and the CMS Information Security Handbook.

V. Effects of the Modified System of Records on Individual Rights

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CMS will take precautionary measures to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights of patients whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure from the proposed system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act. CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of the disclosure of information relating to individuals.

Dated: November 7, 2007.

Charlene Frizzera,

Chief Operating Officer, Centers for Medicare & Medicaid Services.

SYSTEM NO. 09–70–0529

SYSTEM NAME:

''Employee Building Pass File (EBPF),'' HHS/CMS/OOM.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

The Centers for Medicare & Medicaid Services (CMS) Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850 and at various other contractor locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system contains information on Federal employees, contractors, consultants or grantees, Government Services Administration employees, and contract guards working in CMS's central office complex in Baltimore, Maryland, and other CMS and HHS Federal buildings.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains the name of the employee or other authorized individuals, social security number (SSN), identification card number, building/work location, phone number, position, title, grade, supervisor's name and telephone number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of this system of records is given under Section 5 United States Code (U.S.C.) 301, 40 USCA 121(c)(2), and 41 Code of **Federal Register** (CFR) 102–74.375.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the SOR is to issue and control United States Government building passes issued to all CMS employees and non-CMS employees who require continuous access to CMS buildings in Baltimore and other CMS and HHS facilities. Information retrieved from this SOR will be used to: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or grantee; (2) assist other Federal agencies with activities related to this system; and (3) support litigation involving the Agency.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OR USERS AND THE PURPOSES OF SUCH USES:

A. The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a ''routine use.'' The proposed routine uses in this system meet the compatibility requirement of the Privacy Act. We are proposing to establish the following routine use disclosures of information maintained in the system:

1. To Agency contractors, consultants, or grantees who have been contracted by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system and who need

to have access to the records in order to assist CMS.

2. To assist other Federal agencies with activities related to this system and who need to have access to the records in order to perform the activity.

3. To the Department of Justice (DOJ), court or adjudicatory body when

a. the Agency or any component thereof; or

b. any employee of the Agency in his or her official capacity; or

c. any employee of the Agency in his or her individual capacity where the DOJ has agreed to represent the employee; or

d. the United States Government;

is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

All records are stored on electronic media.

RETRIEVABILITY:

The collected data are retrieved by an individual identifier; e.g., name or SSN.

SAFEGUARDS:

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources, also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

RETENTION AND DISPOSAL:

CMS will retain information for a total period not to exceed 25 years. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER AND

Director Security & Emergency Management Group, Office of Operations Management, CMS, Room SLL–11–28, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, employee identification number, tax identification number, national provider number, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), HICN, and/or SSN (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay).

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7).

RECORDS SOURCE CATEGORIES:

CMS obtains information in this system from the individuals who are covered by this system.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. E7–22817 Filed 11–21–07; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Submission for OMB Review; Comment Request

Title: Notice of Lien.

OMB No.: 0970–0153.

Description: Section 452(a)(11) of the Social Security Act requires the Secretary of Health and Human Services to promulgate a form for imposition of liens to be used by the State child support enforcement (Title IV–D) agencies in interstate cases. Section 454(9)(E) of the Social Security Act requires each State to cooperate with any other State in using the Federal form for imposition of liens in interstate child support cases. Tribal IV–D agencies are not required to use this form but may choose to do so. OMB approval of this form is expiring in January 2008 and the Administration for Children and Families is requesting an extension of this form.

Respondents: State, local or Tribal agencies administering a child support enforcement program under title IV–D of the Social Security Act.

ANNUAL BURDEN ESTIMATES

Instrument	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
Notice of Lien	123,637	1	.25	30,909
Estimated Total Burden Hours:				30,909