Prevention (CDC), and the Director, National Centers for Injury Prevention and Control (NCIPC) regarding feasible goals for the prevention and control of injury. The committee makes recommendations regarding policies, strategies, objectives, and priorities, and reviews progress toward injury prevention and control.

Matters to be Discussed: The meeting will open to the public. The Advisory Committee for Injury Prevention and Control (ACIPC) will be discussing partnership activities and how the ACIPC can advance the field of injury prevention and control. Agenda items are subject to change as priorities dictate.

Contact Person for More Information: Ms. Amy Harris, Executive Secretary, ACIPC, NCIPC, CDC, 4770 Buford Highway, NE., M/S K61, Atlanta, Georgia 30341–3724, telephone (770) 488–4936.

The Director, Management Analysis and Services Office, has been delegated the authority to sign **Federal Register** notices pertaining to announcements of meetings and other committee management activities, for both CDC and the Agency for Toxic Substances and Disease Registry.

Dated: November 5, 2007.

Elaine L. Baker,

Director, Management Analysis and Services Office, Centers for Disease Control and Prevention.

[FR Doc. E7–22149 Filed 11–9–07; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Board of Scientific Counselors, National Institute for Occupational Safety and Health (BSC, NIOSH)

In accordance with section 10(a)(2) of the Federal Advisory Committee Act (Pub. L. 92–463), the Centers for Disease Control and Prevention (CDC) announces the following meeting for the aforementioned committee:

Time and Date: 10 a.m.–2 p.m., December 13, 2007.

Place: Holiday Inn Capitol, 550 C Street, SW., Washington, DC 20024.

Status: Open to the public, limited only by the space available. The meeting room accommodates approximately 50 people. Teleconference available toll-free; please dial (888) 677–1819, Participant Pass Code 25404.

Purpose: The Secretary, the Assistant Secretary for Health, and by delegation the Director, Centers for Disease Control and Prevention, are authorized under sections 301 and 308 of the Public Health Service Act to conduct directly or by grants or contracts, research, experiments, and demonstrations relating to occupational safety and health and to mine health. The Board of Scientific Counselors shall provide guidance to the Director, National Institute for Occupational Safety and Health on research and prevention programs. Specifically, the Board shall provide guidance on the Institute's research activities related to developing and evaluating hypotheses, systematically documenting findings and disseminating results. The Board shall evaluate the degree to which the activities of the National Institute for Occupational Safety and Health: (1) Conform to appropriate scientific standards, (2) address current, relevant needs, and (3) produce intended results.

Matters To Be Discussed: NIOSH Response to the National Academies of Science Program Reviews.

Agenda items are subject to change as priorities dictate.

For Further Information Contact: Roger Rosa, Executive Secretary, BSC, NIOSH, CDC, 395 E Street, SW., Suite 9200, Patriots Plaza Building, Washington, DC 20201, telephone (202) 245–0655, fax (202) 245–0664.

The Director, Management Analysis and Services Office, has been delegated the authority to sign **Federal Register** notices pertaining to announcements of meetings and other committee management activities for both the CDC and the Agency for Toxic Substances and Disease Registry.

Dated: November 5, 2007.

Elaine L. Baker,

Director, Management Analysis and Services Office, Centers for Disease Control and Prevention (CDC).

[FR Doc. E7–22155 Filed 11–9–07; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

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

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

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

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify an existing SOR titled, ''Individuals Authorized Access to Centers for Medicare & Medicaid Services (CMS) Computer Services (IACS), System No. 09–70–0064,'' most recently modified at 67 *FR* 48911 (July 26, 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 identifying number for this system should read: System No. 09–70–0538.

We propose to broaden the scope of this system to include a CMS service planned to provide a centralized user provisioning and administration service that supports the creation, deletion, and lifecycle management of enterprise identities. This service creates accounts, supports Role Based Access Control (RBAC), and provides business application integration points. RBAC is a form flow approval process and enterprise identity audit and recertification based on the role of the individual. The business application integration point allows business application owners to use the form flow process of the user provisioning service to approve or deny requests for access to business applications. This modification will permit CMS to implement a unified framework for managing user information and access rights, for those individuals who apply for and are granted access across multiple CMS systems and business contexts.

We propose to modify existing routine use number 1 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 separate from CMS contractors and/or consultants. The modified routine use will remain as routine use number 1. We will delete routine use number 2 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 system has been to collect and maintain individually identifiable information to assign, control, track, and report authorized access to and use of CMS's computerized information and resources, for those individuals who apply for and are granted access across multiple CMS systems and business contexts. Information in this system will also be used to: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or CMS grantee; and (2) support litigation involving the Agency related to this system. We have provided background information about the modified system in the ''Supplementary Information'' section below. Although the Privacy Act requires only that the ''routine use'' portion of the system be published for comment, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

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 7, 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: Nancy Martin, Division of Development & Engineering, Information Services Design & Development Group, Office of Information Services, CMS, Room N2–15–04, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Her telephone number is 410–786–0167, or e-mail at *Nancy.Martin@cms.hhs.gov*.

SUPPLEMENTARY INFORMATION: The IACS framework consists of two major components: An identity management service and a set of authentication or access management services. These two components will enable a single identity to be used throughout CMS and will ensure that users authenticate to applications using a level of assurance equal to the sensitivity of the application and/or data. As CMS moves into the web-enabled application arena for mission critical applications, the need to securely manage this environment is a major concern. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements, e-Authentication guidance and the Personal Identity Verification initiative make the need for a security services framework even more important.

CMS has provided an application that will streamline our information technology environment so that existing and new applications can work more effectively by sharing information, and so that CMS can be more responsive to the demands of changing business needs and emerging technology. CMS plans to make our data more readily accessible to our beneficiaries, partners, and stakeholders in a secure, efficient, and carefully planned manner. In striving to meet these goals, CMS has established a target enterprise architecture and modernization strategy that is based upon several key design principles: (1) An established, secure Internet architecture for the CMS enterprise; (2) Defined products for the target enterprise architecture; (3) Defined security classifications and controls for CMS applications; (4) Defined security services that support the architecture and implement the controls; and (5) Prescriptive application development standards and guidelines for the target environment.

When an account/identity is created, a unique identifier will be generated to universally associate a user with CMS. The provisioning service uses a seven-character algorithm to generate user IDs that are unique across the CMS enterprise. The provisioning service will also provide a mechanism to assign roles that will be maintained in the central data store. An application integration point will be established to allow business application owners to use the user provisioning service to approve or deny requests for access to business applications.

Initial users of the IACS will be primarily CMS business partners such as health care plans and customer inquiry service personnel who answer queries to 1–800–MEDICARE. Three entities are key in providing this support: The Customer Support for Medicare Modernization Support, the CMS IT CITIC Service Desk and the Centers for Beneficiary Choices. Future users will consist of but are not limited to, individuals who apply from Plans and Providers, Provider Hospitals, Group Practitioners, Physicians and Beneficiaries.

I. Description of the Modified System of Records

A. Statutory and Regulatory Basis for the System

Authority for maintenance of the system is given under Executive Order 9397, the Debt Collection Improvement Act, 31 United States Code (U.S.C.) § 7701(c)(1), and 5 U.S.C. 552a(b)(1).

B. Collection and Maintenance of Data in the System

Information for this system is collected and maintained on individuals who voluntarily apply for access to the Web-based Application Systems and individuals with an approved need for access to the computer resources and information maintained by CMS. Information collected for this system will include, but is not limited to, name, social security number, date of birth, current Resource Access Control Facility Identification (RACF ID), e-mail address, telephone number, company name, and geographic location.

II. Agency Policies, Procedures, and Restrictions on the Routine Use

A. Agency Policies, Procedures, and Restrictions on the Routine Use

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 IACS 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 collect the minimum personal data necessary to achieve the purpose of IACS. CMS has the following policies and procedures concerning disclosures of information that will be

maintained in the system. Disclosure of information from the system 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 that the data is being collected, e.g., to collect and maintain individually identifiable information to assign, control, track, and report authorized access to and use of CMS's computerized information and resources.

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. 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 support Agency contractors, consultants, or CMS grantee 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 grantee 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 grantee 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 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.

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 modified 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.: 09–70–0538

SYSTEM NAME:

''Individuals Authorized Access to Centers for Medicare & Medicaid Services (CMS) Computer Services (IACS), HHS/CMS/OIS''.

SECURITY CLASSIFICATION:

Level 3 Privacy Act Sensitive.

SYSTEM LOCATION:

Centers for Medicare & Medicaid Services Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Information for this system is collected and maintained on individuals who voluntarily apply for access to the Web-based Application Systems and individuals with an approved need for access to the computer resources and information maintained by CMS.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information collected for this system will include, but is not limited to, name, social security number (SSN), date of birth, current Resource Access Control Facility Identification (RACF ID), e-mail address, telephone number, company name, and geographic location.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under Executive Order 9397, the Debt Collection Improvement Act, 31 United States Code (U.S.C.) § 7701(c)(1), and 5 U.S.C. 552a(b)(1).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the system has been to collect and maintain individually identifiable information to assign, control, track, and report authorized access to and use of CMS's computerized information and resources, for those individuals who apply for and are granted access across multiple CMS systems and business contexts. Information in this system will also be used to: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or CMS grantee; and (2) support litigation involving the Agency related to this system.

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 support Agency contractors, consultants, or CMS grantee 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 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.

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

STORAGE:

All records are stored on magnetic media.

RETRIEVABILITY:

Information can be retrieved by assigned User ID, user name, and user e-mail address.

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.

RETENTION AND DISPOSAL:

CMS will retain information for the duration the user needs access to CMS' computer systems or until no longer needed for administrative, legal, audit or other operations services, whichever is longer. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER AND ADDRESS:

Director, Division of Development & Engineering, Information Services Design & Development Group, Office of Information Services, CMS, Mail Stop N2–15–18, 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, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and 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.)

RECORD SOURCE CATEGORIES:

Sources of information contained in this records system include data collected from applications submitted by the individuals requiring access to computer services.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. E7–22079 Filed 11–9–07; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

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

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 titled ''Home Health Agency (HHA) Outcome and Assessment Information Set (OASIS),'' System No. 09–70–9002, last modified at 66 **Federal Register** 66903 (December 27, 2001). 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. 09–70–0522.

We propose to modify existing routine use number 1 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 separate from CMS contractors and/or consultants. The modified routine use will remain as routine use number 1. We will modify existing routine use number 4 that permits disclosure to Peer Review Organizations (PRO). Organizations previously referred to as PROs will be renamed to read: Quality Improvement Organizations (QIO). Information will be disclosed to QIOs relating to assessing and improving HHA quality of care. The modified routine use will remain as routine use number 4.

CMS proposes to broaden the scope of the disclosure requirement for routine use number 5, authorizing disclosure to national accrediting organizations that have been approved by CMS for deeming authority for Medicare requirements for home health services. Information will be released to these organizations for only those facilities that they accredit and that participate in the Medicare program and if they meet the following requirements: (1) Provide identifying information for HHAs that have an accreditation status with the requesting deemed organization, (2) submission of a finder file identifying beneficiaries/patients receiving HHA services, (3) safeguard the confidentiality of the data and prevent unauthorized access, and (4) upon completion of a signed data exchange agreement or a CMS data use agreement.

We will delete routine use number 7 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. We will broaden the scope of published routine uses number 8 and 9, authorizing disclosures to combat fraud and abuse in the Medicare and Medicaid programs to include combating ''waste'' which refers increasingly more to specific beneficiary or recipient practices that result in unnecessary cost to Federally-funded health benefit programs.

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 purposes of the SOR are to collect and maintain information to: (1) Study and help ensure the quality of care provided by home health agencies (HHA); (2) aid in administration of the survey and certification of Medicare/Medicaid HHAs; (3) enable regulators to provide HHAs with data for their internal quality improvement activities; (4) support agencies of the state government to determine, evaluate and assess overall effectiveness and quality of HHA services provided in the state; (5) provide for the validation, and refinements of the Medicare Prospective Payment System; (6) aid in the administration of Federal and state HHA programs within the state; and (7) monitor the continuity of care for patients who reside temporarily outside of the state. Information maintained in this system will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor, consultant, or grantee; (2) assist another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations; (3) support research, evaluation, or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects; (4) support the functions of Quality Improvement Organizations (QIO); (5) support the functions of national accrediting organizations; (6) support litigation involving the Agency; (7) combat fraud, waste, and abuse in certain health care programs. 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 routine uses, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

EFFECTIVE DATES: CMS filed a modified or altered system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Homeland Security & Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on November 6, 2007. To ensure that all parties have adequate time in which to comment, the modified system, including routine uses, will become effective 30 days from the publication of the notice, or 40 days from the date it was submitted to OMB and 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