will be deleted or overwritten using overwriting software that wipes the entire physical disk and not just the virtual disk. Overwriting is required for the destruction of all electronic SBU information.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Select Agents and Toxins, Coordinating Office for Terrorism Preparedness and Emergency Response, Bldg. 20, Rm. 4100, MS A46, Centers for Disease Control and Prevention, 1600 Clifton Road, NE., Atlanta, GA 30333.

NOTIFICATION PROCEDURE:

An individual may learn if a record exists about himself or herself by contacting the system manager at the above address. Requesters in person must provide driver's license or other positive identification. Individuals who do not appear in person must submit a notarized request on institutional letterhead to verify their identity. The knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act subject to a $5,000 fine and/or imprisonment.

RECORD ACCESS PROCEDURES:

Same as notification procedures. Requestors should also reasonably specify the record contents being sought. An accounting of disclosures that have been made of the record, if any, may also be requested.

CONTESTING RECORD PROCEDURES:

Contact the system manager at the address specified above, reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

RECORD SOURCE CATEGORIES:

Applicants registering for possession, use, and transfer of select agents and the U.S. Attorney General.

[FR Doc. E7–12682 Filed 6–29–07; 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 New System of Records

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

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

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system titled, ''Medicare Master Death Records File (MMDRF), System No. 09–70–0597.'' Under the provisions of Sections 1106 (42 U.S.C. 1306 and 205(r) (42 U.S.C. 405(r) of the Social Security Act (the Act), the Social Security Administration (SSA) will provide to CMS the SSA Death Master File including unrestricted State death data. CMS will use this death data to: (1) Ensure that no future payments are made to any physician or individually enrolled practitioner and other individuals for whom CMS has a record of death, and (2) investigate and initiate an appropriate response where a deceased physician's billing number has been found to have been used as the basis for a request for payment for services allegedly rendered after the physician's date of death. Upon independent verification of the facts with respect to specific individuals, the results will be used to update CMS databases and may also be used to support payment recovery operations and or the work of law enforcement. We have provided additional background information about the new system in the ''Supplementary Information'' section below.

The primary purpose of this system is to collect and maintain Social Security Administration death records for physicians, non-physician practitioners and individuals associated with organizational providers and suppliers to ensure payments are not made for services rendered after confirmed date of death and to prevent and/or detect any fraud, waste and abuse. Information retrieved from this system may be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant, CMS grantee; (2) assist another Federal or State agency with information to contribute to the accuracy of CMS's proper payment of Medicare benefits, enable such agency to administer a Federal health benefits program, or to enable such agency to fulfill a requirement of Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; (3) support litigation involving the agency; and (4) combat fraud, waste, and abuse in certain Federally-funded health benefits programs.

EFFECTIVE DATES: CMS filed a new system report with the Chair of the House Committee on Oversight and Government Reform, 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 *June 25, 2007.* To ensure that all parties have adequate time in which to comment, the new 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. 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.

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: Allen Gillespie, Technical Advisor, Division of Provider/Supplier Enrollment, Program Integrity Group, Office of Financial Management, Mail Stop C3–24–01, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244–1849. He can be reached by telephone at 410–786–5996, or via e-mail at *allen.gillespie@cms.hhs.gov.*

SUPPLEMENTARY INFORMATION: CMS staff will develop a program to compare data on the monthly MMDRF with individuals in the Provider Enrollment Chain Ownership System (PECOS). A report of potential matches from the MMDRF and PECOS will be distributed monthly to the Parts A and B MACs and affiliated contractors. CMS will issue manual instructions with procedures contractors should follow to determine if the individual name on the monthly report is a match to the individual in the

PECOS database. When contractors verify there is a match there will be additional procedures for updating PECOS and, in turn, the corresponding claims systems.

I. Description of the Proposed System of Records

A. Statutory and Regulatory Basis for SOR

The statutory authority for maintenance of this system is given under the provisions of Sections 1106 (42 U.S.C. 1306) and 205(r) (42 U.S.C. 405(r)) of the Social Security Act (the Act).

B. Collection and Maintenance of Data in the System Information is collected on all providers with a Social Security number (SSN) whose death has been reported to the Social Security Administration or to CMS, and the death has not been verified. The system will comprise death records about providers who participate in the Medicare program. Examples include, but are not limited to: name, SSN, demographic information, unique provider identification number, National Provider Identifier (NPI), etc.

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 MMDRF information that can be associated with an individual as prt will only release MMDRF 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 MMDRF.

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 Social Security Administration death records for physicians, non-physician practitioners and individuals associated with organizational providers and suppliers to ensure payments are not made for services rendered after confirmed date of death and to prevent and/or detect any fraud, waste and abuse.

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. Routine Uses of Data

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 engaged by the agency to assist in the performance of a service related to this collection and who need to have access to the records in order to perform the activity.

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 function relating to purposes for this system.

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

2. To another Federal or State agency to:

a. Contribute to the accuracy of CMS's proper payment of Medicare benefits;

b. Enable such agency to administer a Federal health benefits program, or, as necessary, to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; and/or

c. Assist Federal/state Medicaid programs within the State.

Other Federal or State agencies, in their administration of a Federal health program, may require MMDRF information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided.

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, and occasionally when another party is involved in litigation and CMS 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.

4. To a CMS contractor that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct,

remedy, or otherwise combat fraud, waste, or abuse in such program.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual, grantee, cooperative agreement or consultant relationship with a third party to assist in accomplishing CMS functions relating to the purpose of combating fraud and abuse. CMS occasionally contracts out certain of its functions or makes grants or cooperative agreements when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor, grantee, consultant or other legal agent whatever information is necessary for the agent to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the agent from using or disclosing the information for any purpose other than that described in the contract and requiring the agent to return or destroy all information.

5. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate potential fraud, waste, or abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs.

Other agencies may require MMDRF information for the purpose of combating fraud, waste, and abuse in such Federally-funded programs.

IV. Protections

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.

V. Effects 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 this 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 information relating to individuals.

Dated: June 20, 2007.

Charlene Frizzera,

Chief Operating Officer, Centers for Medicare & Medicaid Services.

SYSTEM NO. 09–70–0597

SYSTEM NAME:

''Medicare Master Death Records File (MMDRF),'' HHS/CMS/OFM.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Information is collected on all providers with a Social Security number (SSN) whose death has been reported to the Social Security Administration or to CMS, and the death has not been verified. The system will comprise death records about providers who participate in the Medicare program.

CATEGORIES OF RECORDS IN THE SYSTEM:

The collected information will include, but is not limited to: name, SSN, demographic information, unique provider identification number, National Provider Identifier (NPI), etc.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The statutory authority for maintenance of this system is given under the provisions of Sections 1106 (42 U.S.C. 1306) and 205(r) (42 U.S.C. 405(r)) of the Social Security Act (the Act).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of this system is to collect and maintain Social Security Administration death records for physicians, non-physician practitioners and individuals associated with organizational providers and suppliers to ensure payments are not made for services rendered after confirmed date of death and to prevent and/or detect any fraud, waste and abuse. Information retrieved from this system may be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant, CMS grantee; (2) assist another Federal or State agency with information to contribute to the accuracy of CMS's proper payment of Medicare benefits, enable such agency to administer a Federal health benefits program, or to enable such agency to fulfill a requirement of Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; (3) support litigation involving the agency; and (4) combat fraud, waste, and abuse in certain Federally-funded health benefits programs.

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 engaged by the agency to assist in the performance of a service related to this collection and who need to have access to the records in order to perform the activity.

2. To another Federal or State agency to:

a. Contribute to the accuracy of CMS's proper payment of Medicare benefits;

b. Enable such agency to administer a Federal health benefits program, or, as necessary, to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; and/or

c. Assist Federal/state Medicaid programs within the state.

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.

4. To a CMS contractor that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

5. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

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 the name or other identifying information of the physician/practitioner, health care provider.

PROTECTIONS:

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 identifiable information maintained in the MMDRF system of records for a period of 6 years 3 months. 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 Provider/Supplier Enrollment, Program Integrity Group, Office of Financial Management, Mail Stop C3–24–01, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244–1849.

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), NPI, 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

Data will be collected from beneficiary enrollment records, provider enrollment records, and the Death Master File including unrestricted State death data provided by the Social Security Administration.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT

None.

[FR Doc. E7–12677 Filed 6–29–07; 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 of Records

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