Due to programmatic matters, this **Federal Register** Notice is being published on less than 15 calendar days notice to the public (41 CFR 102–3.150(b)).

Contact Person for More Information: Shirley D. Little, Committee Management Specialist, Office of Science, NCEH/ATSDR, 1600 Clifton Road, NE., M/S E–28, Atlanta, Georgia 30333, telephone 404–498–0615.

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 NCEH/ATSDR.

Dated: November 14, 2006.

Alvin Hall,

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

[FR Doc. E6–19544 Filed 11–17–06; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Public Health Security and Bioterrorism Preparedness and Response Act Delegation of Authority

Notice is hereby given that I have delegated to the Director, Centers for Disease Control and Prevention (CDC), with authority to redelegate, the following authorities vested in the Secretary of Health and Human Services, under Title III of the Public Health Service (PHS) Act and the Public Health Security and Bioterrorism Preparedness and Response (PHSBPR) Act of 2002 (Pub. L. 107–188) as amended hereafter, insofar as these authorities pertain to the functions assigned to the CDC:

- PHS Act, Title III, Section 351A (42 U.S.C. 262a), excluding sections (i), (g)(3) and (g)(4) as provided in § 201 of the Act; and
- PHSBPR Act, Title II, Subtitle C, Section 221 (7 U.S.C. 8411).

This delegation excludes the authority to submit reports to the Congress, but should be exercised under the Department's existing delegation of authority and policy on regulations.

This delegation is effective upon signature. In addition, I hereby affirm and ratify any actions taken by you or your subordinates which involved the exercise of the authorities delegated herein prior to the effective day of the delegation.

Dated: November 8, 2006.

Michael O. Leavitt,

Secretary.

[FR Doc. 06–9263 Filed 11–17–06; 8:45 am]

BILLING CODE 4160–18–M

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 existing SOR, ''Record of Individuals Authorized Entry to the Health Care Financing Administration (HCFA) Building via a Card Key Access System (RICKS), System No. 09–70–3001'' last modified 66 FR 15264 (March 16, 2001). The name of the Agency has been changed from HCFA to the Centers for Medicare & Medicaid Services (CMS). We will modify the system name to read: ''Record of Individuals Authorized Entry to the CMS Building via a Card Key Access System (RICKS).'' 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 HCFA systems of records. The new assigned identifying number for this system should read: System No. 09–70–0518.

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 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.

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 of records is to issue and control United States Government card keys to all CMS employees and other authorized individuals who require access into certain designated or secured areas. Information retrieved from this system of records 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 agency to conduct 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 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 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 13, 2006. 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, MD 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 Resources Management and Response Group, Office of Operations Management, CMS, Room SLL–11–08, CMS, 7500 Security Boulevard, Baltimore, MD 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 System

The authority for this system is given under the provisions of 5 United States Code (U.S.C.) 301, 40 U.S.C. 121, 41 Code of Federal Regulations (CFR) Part 102–74, Subpart C (Conduct on Federal Property), 5 U.S.C. 552a(e)(10), and Office of Management and Budget Circular A–123, ''Internal Control Systems.''

B. Collection and Maintenance of Data in the System

The system collects and maintains information on Federal employees, contractors and consultants, Government Services Administration (GSA) employees, and contract guards working in the central office complex in Baltimore. The information maintained contains the individual's name, assigned card key number, demographic and geographic information, and the building/secure area location. The system also contains the date and time of actual or attempted entry to secured areas.

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

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 RICKS 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 RICKS. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from this 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 information to issue and control United States Government card keys to all CMS employees and other authorized individuals.

2. Determines:

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

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

c. That 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; and

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

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 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 assist another Federal agency to conduct activities related to this system of records 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 another Federal agency to assist in accomplishing CMS functions relating to purposes for this system of records.

The Federal Protection Service may require RICKS information if investigating a crime and/or in the administration of its assigned responsibilities.

3. To support 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.

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 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 of the Modified or Altered System of Records on Individual Rights

CMS proposes to modify 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 (see item IV above) 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 information relating to individuals.

Dated: November 8, 2006.

John R. Dyer,

Chief Operating Officer, Centers for Medicare & Medicaid Services.

SYSTEM NO. 09–70–0518

SYSTEM NAME:

''Record of Individuals Authorized Entry to CMS Building via a Card Key Access System (RICKS), 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 South Building, Baltimore, Maryland 21244–1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system collects and maintains information on Federal employees, contractors and consultants, Government Services Administration (GSA) employees, and contract guards working in the central office complex in Baltimore.

CATEGORIES OF RECORDS IN THE SYSTEM:

The information maintained contains the individual's name, assigned card key number, demographic and geographic information, and the building/secure area location. The system also contains the date and time of actual or attempted entry to secured areas.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The authority for this system is given under the provisions of 5 United States Code (U.S.C.) 301, 40 U.S.C. 121, 41 Code of Federal Regulations (CFR) Part 102–74, Subpart C (Conduct on Federal Property), 5 U.S.C. 552a(e)(10), and Office of Management and Budget Circular A–123, ''Internal Control Systems.''

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the system of records is to issue and control United States Government card keys to all CMS employees and other authorized individuals who require access into certain designated or secured areas. Information retrieved from this system of records 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 agency to conduct activities related to this system; and (3) support litigation involving the agency.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF 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 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 assist another Federal agency to conduct activities related to this system of records and who need to have access to the records in order to perform the activity.

3. To support 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 paper and magnetic disk.

RETRIEVABILITY:

Magnetic media records are retrieved by the name of the employees or other authorized individual and/or card key number. Paper records are retrieved alphabetically by name.

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:

Records are retained for up to 3 years following expiration of an individual's authority to enter secured areas. When an individual is no longer authorized, information is deleted from magnetic media immediately.

SYSTEM MANAGER AND ADDRESS:

Director, Emergency Management and Response 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, assigned card key number, and building/secure area, 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 specify the record contents being sought. (These procedures are in accordance with department regulation 45 CFR 5b.5(a)(2).)

CONTESTING RECORDS PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the records 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:

The data contained in this system of records are obtained from the individuals who submit a request for access to a secure building or area.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. E6–19503 Filed 11–17–06; 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, we are proposing to modify or alter an existing SOR titled, ''Medicare-Cancer Registry Record System (MCR), System No. 09–70–0042,'' established at 53 FR 38082 (September 29, 1988), and most recently modified at 65 FR 37792 (June 16, 2000). 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. 09–70–0509.

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 be renumbered 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.

We propose to broaden the scope of the disclosure provisions of this system by adding a routine use to permit the release of information to another Federal or state agency to contribute to the accuracy of CMS' proper payment of Medicare benefits, to enable such agency to administer a Federal health benefits program, and/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, to evaluate and to monitor the amount and kinds of services received by Medicare beneficiaries contracting cancer. The added routine use will be numbered as routine use number 2.

We will further broaden the scope of this system by including 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'' applies whenever the system collects or maintains PHI. This system may contain PHI. In addition, our policy to prohibit release if there is a possibility that an individual can be identified through ''small cell size'' will apply to the data disclosed from 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