1. To formal third party groups pursuant to agreements with the CMS to pay Medicare premiums on behalf of their members and who need to have access to the records in order to perform the activity.

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent pursuant to agreements with CMS 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 Agency contractors or consultants who have been engaged by the Agency to assist in accomplishment of an CMS function relating to the purposes for this SOR and who have need to have access to the records in order to assist CMS.

4. To an individual or organization for research, evaluation, or epidemiological projects related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.

5. To a Member of Congress or congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

6. 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.

7. To a CMS contractor (including, but not limited to fiscal intermediaries and carriers) 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.

8. 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:

Computer diskette and on magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by name, HICN, and assigned agency identification number.

SAFEGUARDS:

CMS has safeguards for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data.

In addition, CMS has physical safeguards in place to reduce the exposure of computer equipment and thus achieve an optimum level of protection and security for the SPACE system. For computerized records, safeguards have been established in accordance with the Department of Health and Human Services (HHS) standards and National Institute of Standards and Technology guidelines, *e.g.,* security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management Circular #10, Automated Information Systems Security Program; CMS Automated Information Systems Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

RETENTION AND DISPOSAL:

Records are maintained in a secure storage area with identifiers for six years three months after final action of the case is completed.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Premium Billing, Benefits Operations Group, Center for Medicare Management, CMS, 7500 Security Boulevard, S1–06–03, 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, HIC, date of birth, and sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (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:

Information contained in this records system is obtained from third party agencies, Social Security Administration's Master Beneficiary Record, and CMS' Enrollment Database.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–15004 Filed 6–13–02; 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 Modified or Altered System

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) (formerly the Health Care Financing Administration).

ACTION: Notice of 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.'' We propose to delete published routine uses number 1 authorizing disclosures to the Federal Protection Services (FPS), number 2 authorizing disclosures to ''management officials inquiring about an individual's authorization to enter Federal occupied buildings,'' number 3 authorizing disclosures to contractors, and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA). Disclosures allowed by routine use number 1, and to the SSA will be covered by proposed routine use number 2 to permit release of information to ''another Federal agency.'' Routine use number 2 is being deleted because it is not clear what ''management officials'' are being identified and who should receive information referred to in routine use number 2. Disclosures previously allowed by the former routine use number 2 will now be covered by the proposed routine use number 2 and by exceptions to the Privacy Act. Disclosures previously allowed by routine use number 3 will now be covered by proposed routine use number 1.

The security classification previously reported as ''None'' will be modified to reflect that the data in this system is considered to be ''Level Three Privacy Act Sensitive.'' We are modifying the language in the remaining routine uses 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 proposed usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization 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: support regulatory and policy functions performed within the Agency or by a contractor or consultant, assist other Federal agencies with activities related to this system, support constituent requests made to congressional representatives, and 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.

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 Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on May 22, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered 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: Director, Division of Data Liaison and Distribution (DDLD), 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 daylight time.

FOR FURTHER INFORMATION CONTACT: Marcia Levin, Division of Facilities Management Services, Administrative Services Group, CMS, SLL–11–18, 7500 Security Boulevard, Baltimore, Maryland, 21244–1850. The telephone number is 410–786–7840.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Background

In 1981, CMS established this system to carry out the directives authorizing Federal workers and other authorized personnel be issued United States Government identification cards. Notice of this system, ''Employee Building Pass File (EBP) System, System No. 09–70–3002,'' was published in the **Federal Register** (FR) at 46 FR 3524 (Jan. 15, 1981), and modified at 61 FR 6645 (added unnumbered SSA routine use).

B. Statutory and Regulatory Basis for System

Authority for maintenance of this system of records is given under section 486(c) of Title 40, United States Code (USC) and Title 41, Code of Federal Regulations (CFR), Chapter 101–20.302.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system contain information on Federal employees, contractors and consultants, 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 contain 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.

B. 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 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, or consultants who have been engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this SOR 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 a CMS function relating to purposes for this SOR.

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 or consultant 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 or consultant from using or disclosing the information for any purpose other than that described in the contract and requires the contractor or consultant 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 FPS 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 Members of Congress or to congressional staff members in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

Federal employees and other individuals who may be identified in this system sometimes request the help of a Member of Congress in resolving an issue relating to a matter before CMS. The Member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

4. 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 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.

B. Additional Circumstances Affecting Routine Use Disclosures

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 (12–28–00), as amended by 66 FR 12434 (2–26–01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information''.

In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

IV. Safeguards

A. Administrative Safeguards

The EBP system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1984, Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Office and Management and Budget (OMB) Circular A–130, Appendix III, ''Security of Federal Automated Information Resources.'' CMS has prepared a comprehensive system security plan as required by OMB Circular A–130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems. Paragraphs A–C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

Authorized users: Personnel having access to the system have been trained in Privacy Act and systems security requirements. Employees and contractors who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. In addition, CMS is monitoring the authorized users to ensure against excessive or unauthorized use. Records are used in a designated work area or workstation and the system location is attended at all times during working hours.

To insure security of the data, the proper level of class user is assigned for each individual user as determined at the Agency level. This prevents

unauthorized users from accessing and modifying critical data. The system database configuration includes five classes of database users:

• Database Administrator class owns the database objects; *e.g.,* tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;

• Quality Control Administrator class has read and write access to key fields in the database;

• Quality Indicator Report Generator class has read-only access to all fields and tables;

• Policy Research class has query access to tables, but are not allowed to access confidential patient identification information; and

• Submitter class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards

All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the EBP system:

Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information System resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

• *User Log on*—Authentication is performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.

• *Workstation Names*—Workstation naming conventions may be defined and implemented at the Agency level.

• *Hours of Operation*—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the Agency level.

• *Inactivity Log-out*—Access to the NT workstation is automatically logged out after a specified period of inactivity.

• *Warnings*—Legal notices and security warnings display on all servers and workstations.

• *Remote Access Services (RAS)*—Windows NT RAS security handles resource access control. Access to NT resources is controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

C. Procedural Safeguards

All automated systems must comply with Federal laws, guidance, and policies for information systems security as stated previously in this section. Each automated information system should ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

V. Effect of the Modified System 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. We will only disclose the minimum personal data necessary to achieve the purpose of EBP.

Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure. CMS has assigned a higher level of security clearance for the information in this system to provide added security and protection of data in this system.

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. 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: May 22, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–3002

SYSTEM NAME:

Employee Building Pass File (EBP) System, HHS/CMS/OICS.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive.

SYSTEM LOCATION:

Centers for Medicare & Medicaid Services (CMS), 7500 Security Boulevard, North Building, First Floor (magnetic media), and South Building, Lower Level, Baltimore, Maryland 21244–1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The identified individual includes Federal employees, contractors and consultants, and Government Services Administration (GSA) employees, and contract guards working in CMS's central office complex in Baltimore, Maryland.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes the employees' or other individual's name, social security number, identification card number, building/work location, phone number, position, title, grade, and supervisor's name and telephone number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of this system of records is given under section 486(c) of Title 40, United States Code (USC) and Title 41, Code of Federal Regulations (CFR), Chapter 101–20.302.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the system of records 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 system of records will be used to: support regulatory and policy functions performed within the Agency or by a contractor or consultant, assist other Federal agencies with activities related to this system, support constituent requests made to a congressional representative, and support litigation involving the Agency.

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

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 use in this system meets the compatibility requirement of the Privacy Act.

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 (12–28–00), as amended by 66 FR 12434 (2–26–01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information''.

In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary). We are proposing to establish or modify he following routine use disclosures of information which will be maintained in the system:

1. To agency contractors, or consultants who have been engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this SOR 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 Member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

4. 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.

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

STORAGE:

All records are stored on paper and magnetic media.

RETRIEVABILITY:

Magnetic media records are retrieved by the name of the employees or other authorized individuals. Paper records are retrieved alphabetically by name.

SAFEGUARDS:

CMS has safeguards for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data.

In addition, CMS has physical safeguards in place to reduce the exposure of computer equipment and thus achieve an optimum level of protection and security for the EBP system. For computerized records, safeguards have been established in accordance with HHS standards and National Institute of Standards and Technology guidelines, e.g., security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management (IRM) Circular #10, Automated Information Systems Security Program, CMS Automated Information Systems (AIS) Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

RETENTION AND DISPOSAL:

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

SYSTEM MANAGER AND ADDRESS:

Director, Division of Facilities Management Services, Administrative Services Group, Office of Internal Customer Support, CMS, Room SLL–11–08, 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, identification card number, address, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (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:

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. 02–15008 Filed 6–13–02; 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 Modified or Altered System

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) (formerly the Health Care Financing Administration).

ACTION: Notice of 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 a SOR, ''Physician/Supplier 1099 File (Statement for Recipients of Medical and Health Care Payments)(1099), System No. 09–70–0517.'' We propose to delete published routine use number 4 authorizing disclosure to contractors, and an unnumbered routine use