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

authorizing disclosure to the Social Security Administration (SSA). The proposed routine use for contractors and consultants makes material changes to published routine use number 4, and as proposed should be treated as a new routine use. Disclosure of data from this system to the SSA is no longer necessary since SSA has been established as a separate agency outside of the HHS and a routine use for the purpose stated is no longer necessary.

We propose to add two new routine uses to combat fraud and abuse in certain federally funded health care programs. 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 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 provide periodic reporting to the Internal Revenue Service (IRS). Information in this system will also be disclosed to: the IRS, support regulatory and policy functions performed within the agency or by a contractor or consultant, support constituent requests made to a congressional representative, support litigation involving the agency related to this system of records, and combat fraud and abuse in certain federally funded 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 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 30, 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, 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: G. Jeff Chaney, Director, Division of Accounting, Accounting and Risk Management Group, Office of Financial Management, CMS, Room N3–11–17, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–5412. The e-mail address is *gchaney@cms.hhs.gov.*

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Background

In 1980, CMS established a SOR under the authority of the Internal Revenue Code, Title 26 United States Code (USC) sec. 6041. Notice of this system, ''Physician/Supplier 1099 File (Statement for Recipients of Medical and Health Care Payments), HHS/CMS/BPO, System No. 09–70–0517'' was published in the **Federal Register** on Monday, December 22, 1980 (45 FR 84476), 61 FR 6645 (added unnumbered social security use), 63 FR 50552 (added three fraud and abuse uses), and 65 FR 50552 (deleted one and modified two fraud and abuse uses).

B. Statutory and Regulatory Basis for SOR

Authority for the maintenance of this SOR is given under the Internal Revenue Code, Title 26 United States Code (USC) sec. 6041.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system contains information on total Medicare payments that have been made to physicians and suppliers by Medicare carriers and intermediaries. It contains the name, address, assigned provider number, employer identification number (EIN), and social security number (SSN) of the physicians and suppliers.

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 which 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 1099 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 1099. CMS has the following policies and procedures concerning disclosures of information which will be maintained in the system. In general, disclosure of information from the system of records will be approved only for the minimum information necessary to accomplish the purpose of the disclosure only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, e.g., to provide periodic reporting to the IRS.

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 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;

b. Remove or destroy at the earliest time all individually-identifiable information; andgree 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 1099 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 the Internal Revenue Service in connection with the determination of the individual's self-employment income.

We contemplate disclosing information under this routine use only in situations in which the IRS requires 1099 data to assist in the implementation and maintenance of the IRS code.

2. 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.

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.

Individuals sometimes request the help of a Member of Congress in resolving issues 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 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.

5. 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.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contract or grant 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 when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or grantee whatever information is necessary for the contractor or grantee to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or grantee from using or disclosing the information for any purpose other than that described in the contract and requiring the contractor or grantee to return or destroy all information.

6. 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.

Other agencies may require 1099 information for the purpose of combating fraud and abuse in such federally funded programs.

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 1099 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 1099 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 1099. 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 30, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0517

SYSTEM NAME:

Physician/Supplier 1099 File (Statement for Recipients of Medical and Health Care Payments)(1099), HHS/CMS/OFM.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive

SYSTEM LOCATION:

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system contains information on total Medicare payments that have been made to physicians and suppliers by Medicare carriers and intermediaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains the name, address, assigned provider number, employer identification number (EIN), and social security number (SSN) of the physicians and suppliers.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for the maintenance of this SOR is given under the Internal Revenue Code, Title 26 United States Code (USC) sec. 6041.

PURPOSE(S):

The primary purpose of the SOR is to provide periodic reporting to the Internal Revenue Service (IRS). Information in this system will also be disclosed to: the IRS, support regulatory and policy functions performed within the agency or by a contractor or consultant, support constituent requests

made to a congressional representative, support litigation involving the agency related to this system of records, and combat fraud and abuse in certain federally funded health care programs.

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

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 EDB 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. 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).

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 **Federal Register** (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.'' We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To the Internal Revenue Service in connection with the determination of the individual's self-employment income.

2. 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.

3. To a 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

5. 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.

6. 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 maintained in this system can be retrieved by the name, SSN, EIN, and an assigned physician/supplier 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 1099 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 (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 maintained in a secure storage area with identifiers for 5 years.

SYSTEM MANAGER(S) AND ADDRESSES

Director, Division of Accounting, Accounting and Risk Management Group, Office of Financial Management, CMS, Room N3–11–17, 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, address, 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:

The record of the total annual payments made to each physician or supplier is derived from the individual Medicare bill payments.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–15009 Filed 6–13–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 01N–0590]

Agency Information Collection Activities; Submission for OMB Review; Comment Request; Salmonella Discovery System Pilot Study

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA) is announcing that the proposed collection of information listed below has been submitted to the Office of Management and Budget (OMB) for review and clearance under the Paperwork Reduction Act of 1995.

DATES: Submit written comments on the collection of information by July 15, 2002.

ADDRESSES: Submit written comments on the collection of information to the Office of Information and Regulatory Affairs, OMB, New Executive Office Bldg., 725 17th St. NW., rm. 10235, Washington, DC 20503, Attn: Stuart Shapiro, Desk Officer for FDA.

FOR FURTHER INFORMATION CONTACT: Karen L. Nelson, Office of Information Resources Management (HFA–250), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301–827–1482.

SUPPLEMENTARY INFORMATION: In compliance with 44 U.S.C. 3507, FDA has submitted the following proposed collection of information to OMB for review and clearance.

Salmonella Discovery System Pilot Study

FDA's Center for Drug Evaluation and Research, Office of Pharmaceutical Science, Informatics and Computational Safety Analysis Staff intends to conduct a *Salmonella* Discovery System Pilot Study (the pilot study). The primary goal of the pilot study is to construct and execute a mutually beneficial process by which FDA and pharmaceutical companies can share information based on their proprietary toxicology study data and thereby expand their own knowledge databases. This process will be designed and conducted using procedures that do not compromise the identity and chemical structures of the individual collaborator's proprietary chemicals.

The three major objectives of the pilot study are to:

• Build a joint and comprehensive FDA/pharmaceutical industry database for compounds tested in the *Salmonella typhimurium* reverse mutagenicity assay;

• Use these data to construct a new enhanced *Salmonella t.* mutagenicity assay database module for the MultiCASE quantitative structure activity relationship software program; and

• Employ the recently developed MultiCASE expert system (MCASE–ES) to predict the mutagenic response, mutagenic potency, and mechanism of mutagenesis of test chemicals in *Salmonella t.*

The pilot study will be a joint venture designed to maximize the benefits and minimize the risks to all collaborators. FDA intends to send letters to companies that have purchased either MultiCASE or CASETOXII software programs to invite them to become a collaborator in the project.

FDA intends to request that each collaborator submit the following data electronically: (1) Test compound chemical structures; and (2) assay data, identifying the type of *Salmonella* mutagenicity assay used in the studies, the source and concentration of any exogenous activation system used, and the average number of revertants/plate for the negative control, positive control, and each of the test compound treatment groups. Although there is no minimum requirement for the number of test compounds to be submitted to FDA, the agency would expect to receive at least 200 compounds from each collaborator. Each company will be able to identify its own compounds in the resulting discovery system, and the more data submitted, the greater the coverage will be for each company's molecular universe.

FDA intends to act as the broker for the pilot study and will be responsible for the confidentiality and integrity of each collaborator's proprietary data. The number of compounds in the database module will depend upon the number of collaborators and the size of the data sets they contribute to the pilot study. After the enhanced *Salmonella* discovery system has been constructed and tested, FDA intends to custom prepare individual discovery systems for each collaborator.

The anticipated benefits to collaborators include:

• Receipt of a new expanded *Salmonella in silico* discovery tool at no cost;

• Access to proprietary molecular fragment data derived from *Salmonella t.* mutagenicity studies from FDA and other collaborator archives;

• Comprehensive lists of molecular structural alerts correlated with mutagenicity in *Salmonella t.*, including previously uncharacterized alerts derived from heretofore inaccessible undeveloped lead pharmaceutical test data; and

• A *Salmonella* discovery system which should provide high coverage and high predictive performance for organic chemicals in each company's combinatorial and lead chemical data sets.

The *Salmonella* discovery system provided by FDA will be compatible with each company's current MCASE software program currently v. 3.46 and will supplement current *Salmonella* modules purchased from MultiCASE, Inc.

Participation in this pilot study will be voluntary. FDA estimates that approximately 12 companies will participate, and that it will take each company approximately 8 hours to compile the information from electronic archives and submit the requested data and information.

FDA estimates the burden of this collection of information as follows: