provisions set forth in section 552b(c)(4) and (6), Title 5 U.S.C., and the Determination of the Director, Management Analysis and Services Office, CDC, pursuant to Public Law 92–463.

*Matters To Be Discussed:* The meeting will include the review, discussion, and evaluation of applications received in response to RFA OH–02–004.

**CONTACT PERSON FOR MORE INFORMATION:** Pervis Major, Ph.D., Scientific Review Administrator, National Institute for Occupational Safety and Health, CDC, 1095 Willowdale Road, M/S B228, telephone (304) 285–5979.

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

Dated: February 20, 2002.

**Alvin Hall,**

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

[FR Doc. 02–4508 Filed 2–25–02; 8:45 am]

**BILLING CODE 4163–19–P**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

## Centers for Medicare and Medicaid Services

## Privacy Act of 1974; Report of New System

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

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

**SUMMARY:** In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system of records, called the ''Medicare Exclusion Database (MED),'' HHS/CMS/OFM/ No. 09–70–0534. The primary purpose of this system of records is to retrieve information that will be used to aid in the ability of CMS and its contractors (private insurance companies contracted to receive, check and pay bills submitted by providers of services) to ensure that no Medicare payments are made with respect to any item or service (other than an emergency item or service) furnished by an individual or entity during the period when such individual or entity is excluded from participation in Medicare. The information retrieved from this system of records will be used to support regulatory, reimbursement, and policy functions performed within the agency or by a contractor or consultant; 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, or 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; support constituent requests made to a Congressional representative; support litigation involving the agency; and support research, evaluation, and for payment related projects; and to disclose individual-specific information for the purpose of combating fraud and abuse in health benefits programs administered by CMS.

We have provided background information about the proposed system in the **SUPPLEMENTARY INFORMATION** section below. Although the Privacy Act requires only that the ''routine use'' portion of the system be published for comment, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

**EFFECTIVE DATES:** CMS filed a new 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 February 12, 2002. In any event, we will not disclose any information under a routine use until 40 days after publication. We may defer implementation of this system of records or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

**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 time zone.

**FOR FURTHER INFORMATION CONTACT:** Angela Brice-Smith (410) 786–4340, Office of Financial Management, CMS, and 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

**SUPPLEMENTARY INFORMATION:**

### I. Description of the New System of Records

*Statutory and Regulatory Basis for System of Records*

Under sections 1128 A and B and 1156 of the Social Security Act the Department of Health and Human Services through the Office of the Inspector General (OIG) was given the authority to Exclude certain individuals and entities from participation in the Medicare and other Federal and State health care programs. The Medicare contractors are responsible for ensuring that no payment is made with respect to any item or service (other than an emergency item or service) furnished by an individual or entity during the period when such individual or entity is excluded from participation in Medicare. The exclusion also covers orders and referrals for items or services, as well as ownership or management of entities that provide items or services to Medicare beneficiaries.

CMS has recently surveyed the Medicare contractors regarding their ability to successfully enforce OIG exclusions. A number of problems with the current operational process have been identified, some of which directly relate to the data that CMS receives from the OIG and provides to the contractors. The data problems include a lack of standardized format for the cumulative exclusion database, incomplete data, and lack of a process to update exclusion data. Additionally, CMS currently does not have an efficient mechanism to determine which organizations employ excluded individuals.

In order to assist our contractors in determining that no excluded individual or entity receives Medicare payment, CMS will create and maintain a cumulative exclusion database. CMS will be able to match this database against files of providers billing Medicare to ensure that excluded individuals and entities do not violate the terms of their exclusion. In the long term, the MED will be available to a number of users, including all Medicare contractors, the Provider Enrollment Chain and Ownership System (PECOS) and, potentially, Medicaid State Agencies.

The MED project is divided into three phases. Phase I requires that a database be developed, populated and maintained in a standard format which contains the cumulative exclusion database containing all individuals and entities excluded from the Medicare program. The goals of Phase I are to analyze the OIG Exclusion file, clean up

and standardize the data, load a Medicare Exclusion Database (MED) and produce an extract file from the cleaned and standardized data.

Phase II requires that the data from the (MED) database is matched against data from CMS's Online Survey Certification and Reporting System (OSCAR) file, National Supplier Clearinghouse (NSC) file, Unique Physician Identification Number (UPIN) Registry, and Medicare contractor (fiscal intermediaries and carriers) provider files to determine that no excluded individual or entity is doing business with Medicare or Medicare providers and suppliers. Phase II will produce some basic Medicare Exclusion Database reporting for CMS's internal use.

Phase III will involve an open-ended analysis to identify additional tools CMS might use to determine who employs excluded individuals to ensure that employers of excluded individuals are not receiving payments from the Medicare program.

**II. Collection and Maintenance of Data in the System**

*A. Scope of the Data Collected*

The system of records will contain data elements that identify individuals and entities excluded from participation in the Medicare program:

Individual/Entity Name
Unique Physician Identification Number (UPIN)
Date of Birth
SSN
Address
Sanction Type
Sanction Date
Reinstatement Date
Date of Death
Name History
Date of Birth History
Address History
SSN History
UPIN History
EIN History
UPIN Match
OSCAR Match
NSC Match

*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 MED information that can be associated with an individual patient as provided for under ''Section III. Entities Who May Receive Disclosures Under Routine Use.'' Both identifiable and non-identifiable data may be disclosed under a routine use. Identifiable data includes individual records with MED information and identifiers. Non-identifiable data includes individual records with MED information and masked identifiers or MED information with identifiers stripped out of the file.

We will only disclose the minimum personal data necessary to achieve the purpose of the MED. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. In general, disclosure of information from the SOR will be approved only for the minimum information necessary to accomplish the purpose of the disclosure after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected; e.g., developing and refining payment systems and monitoring the quality of care provided to patients.

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

b. Unauthorized use of disclosure of the record;

c. Remove or destroy at the earliest time all patient-identifiable information; and

d. 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 MED 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 the following routine use disclosures of information maintained in the system:

1. To agency contractors, or consultants who have been contracted by the agency to assist in the performance of a service 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 a third party to assist in accomplishing agency business functions relating to purposes for this system of records.

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 whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the contract and requires the contractor to return or destroy all information at the completion of the contract.

2. To the agency of a State Government, or established by State law, for purposes of ensuring that no payments are made with respect to any item or service furnished by an individual or entity during the period when such individual or entity is excluded from participation in Medicare and other Federal and State health care programs.

MED data may potentially be released to the State only on those individuals who are either individuals or entities excluded from participation in the Medicare and other Federal and State health care programs, or employers of excluded individuals or entities, or are legal residents of the State, irrespective of the location of provider or supplier furnishing items or services.

3. To another Federal or State Agency:

a. To contribute to the accuracy of CMS's proper payment of Medicare benefits,

b. To 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.

Other Federal or State agencies in their administration of a Federal health program may require MED information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper payment for services provided. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purpose for which CMS collects the information.

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 for understanding and improving payment projects.

The MED data will provide the research and evaluations a broader, longitudinal, national perspective of the status of individuals that are excluded from participation in Medicare. CMS anticipates that many researchers will have legitimate requests to use these data in projects that could ultimately improve the care provided to Medicare patients and the policy that governs the care. CMS understands the concerns about the privacy and confidentiality of the release of data for a research use.

5. 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.

Beneficiaries sometimes request the help of a Member of Congress in resolving some 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.

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.

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court or adjudicatory body involved. A determination would be made in each instance that, under the circumstances involved, the purposes served by the use of the information in the particular litigation is compatible with a purpose for which CMS collects the information.

7. To a CMS contractor (including, but not necessarily 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 contractual or similar agreement 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 this would contribute to effective and efficient operations. CMS must be able to give a contractor whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards (like ensuring 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 those stated in II.B above), are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the contract and to return or destroy all information.

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.

Other State agencies in their administration of a Federal health program may require MED information for the purpose of preventing, deterring, discovering, detecting, investigating, examining, prosecuting, suing with respect to, defending against, correcting, remedying, or otherwise combating such fraud and abuse in such programs. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purpose for which CMS collects the information.

*B. Additional Provisions Affecting Routine Use Disclosures*

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 System of Records contains Protected Health Information as defined by the Department of Health and Human Services' regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 as amended by 66 FR 12434). 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.''

**IV. Safeguards**

The MED 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 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.

*A. Authorized Users*

Personnel having access to the system have been trained in Privacy Act 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. Records are used in a designated work area and system location is attended at all times during working hours.

To ensure security of the data, the proper level of class user is assigned for each individual user 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 Index 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 will implement 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 CMS system:

Access to all servers is to be 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 is to require 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, which 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 Systems (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-on—Authentication is to be 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 to be determined and implemented at the agency level.
- Inactivity Lockout—Access to the NT workstation is to be automatically locked after a specified period of inactivity.
- Warnings—Legal notices and security warnings are to be displayed on all servers and workstations.
- Remote Access Security—Windows NT Remote Access Service (RAS) security handles resource access control. Access to NT resources is to be 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. These include, but are not limited to: the Privacy Act of 1974; the Computer Security Act of 1987; OMB Circular A–130, revised; Information Resource Management (IRM) Circular #10; HHS Automated Information Systems Security Program; the CMS Information Systems Security Policy, Standards, and Guidelines Handbook; and other CMS systems security policies. 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. Effects of the New 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. 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 monitor the collection and reporting of MED data. MED information is submitted to CMS through standard systems. CMS will utilize a variety of onsite and offsite edits and audits to increase the accuracy of MED data.

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 is 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 maintaining this system of records.

Dated: February 12, 2002.

**Thomas A. Scully,**

*Administrator, Centers for Medicare & Medicaid Services.*

**09–70–0534**

**SYSTEM NAME:**

Medicare Exclusion Database (MED).

**SECURITY CLASSIFICATION:**

Level 3, Privacy Act Sensitive.

**SYSTEM LOCATION:**

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850 and CMS contractors and agents at various locations.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

The system of records will contain data elements that identify individuals and entities excluded from participation in the Medicare program.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

This system of records will contain the individual-level identifying data such as name, addresses, dates of birth and death, Medicare provider identification number, SSN, sanction and reinstatement information, and identifying historical data including name, address, dates of birth, SSN and provider numbers.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Sec. 1128 A and B and 1156 of the Social Security Act.

**PURPOSE(S):**

The primary purpose of this system of records is to retrieve information that will be used to aid in the ability of CMS and its contractors (private insurance companies contracted to receive, check and pay bills submitted by providers of services) to ensure that no Medicare payments are made with respect to any item or service (other than an emergency item or service) furnished by an individual or entity during the period when such individual or entity is excluded from participation in Medicare. The information retrieved from this system of records will be used to support regulatory, reimbursement, and policy functions performed within the agency or by a contractor or consultant; to another Federal or State agency to contribute to the accuracy of CMS's proper payment of Medicare benefits, to enable such agency to administer a Federal health benefits program, or 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; support constituent requests made to a Congressional representative; support litigation involving the agency; and support research, evaluation, and for payment related projects; and to disclose individual-specific information for the purpose of combating fraud and abuse in health benefits programs administered by CMS.

**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 MED 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). Be advised, this System of Records contains Protected Health Information as defined by the Department of Health and Human Services' regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 8462 as amended by 66 FR 12434). 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.''

1. To agency contractors or consultants who have been contracted by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity.

2. To the agency of a State Government, or established by State law, for purposes of ensuring that no payments are made with respect to any item or service furnished by an individual or entity during the period when such individual or entity is excluded from participation in Medicare and other Federal and State health care programs.

3. To another Federal or State agency:

a. To contribute to the accuracy of CMS's proper payment of Medicare benefits,

b. To 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.

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

5. 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.

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 and the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

7. To a CMS contractor (including, but not necessarily 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:**

All records are stored on magnetic, optical and other electronic media

**RETRIEVABILITY:**

The records are retrieved by the Medicare provider number or the National Provider Identifier (NPI).

**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 CMS 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 Information Systems Security, Standards Guidelines Handbook and OMB Circular No. A–130 (revised) Appendix III.

**RETENTION AND DISPOSAL:**

CMS will retain identifiable MED data for a total period of 15 years.

**SYSTEM MANAGER(S) AND ADDRESS:**

CMS, Director, Office of Financial Management/Program Integrity Group, Division of Program Integrity Operations, Health Care Financing Administration, 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, health insurance claim number, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), address, age, and sex, 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 OIG Exclusion file, Online Survey Certification and Reporting System (OSCAR) file, National Supplier Clearing House (NSC) file, Unique Physician Identification Number (UPIN) Registry, Medicare contractor provider files and Social Security Administration (SSA) withholding records or other information services to determine who employs excluded individuals.

**SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:**

None.

[FR Doc. 02–4469 Filed 2–25–02; 8:45 am]

**BILLING CODE 4120–03–P**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Administration for Children and Families

### Submission for OMB review; Comment Request

*Title:* Statewide Automated Child Welfare Information System (SACWIS) Assessment Review GuidE (SARGe).

*OMB No.:* 0970–0159.

*Description:* HHS cannot fulfill its obligation to effectively serve the nation's Adoption and Foster Care populations, nor report meaningful and reliable information to Congress about the extent of problems facing these children or the effectiveness of assistance provided to these populations, without access to timely and accurate information. Currently, SACWIS systems support State efforts to meet the following Federal reporting requirements: the Adoption and Foster Care Analysis and Reporting System (AFCARS) required by section 479(b)(2) of the Social Security Act; the National Child Abuse and Neglect Data System (NCANDS); Child Abuse Prevention and Treatment Act (CAPTA); and the new Chafee Independence Living Program. Forty-seven States and the District of Columbia have developed or have committed to develop a SACWIS system with Federal financial participation. The purpose of these reviews is to ensure that all aspects of the project, as described in the approved Advance Planning Document, have been adequately completed, and conform to applicable regulations and policies.

To initiate a review, States will submit the completed SACWIS Assessment Review GuidE (SARGe) and other documentation at the point that they have completed system development and the system is operational statewide. The additional documents submitted as part of this process should all be readily available to the State as a result of good project management.

The information collected in the SACWIS Assessment Review Guide will allow State and Federal officials to determine if the State's SACWIS system meets the requirements for title IV–E Federal financial participation defined at 45 CFR 1355.50. Additionally, other States will be able to use the documentation provided as part of this review process in their own system development efforts.

*Respondents:* State Title IV–E Agencies.

ANNUAL BURDEN ESTIMATES

| Instrument | Number of respondents | Number of responses per respondent | Average burden hours per response | Total burden hours |
|---|---|---|---|---|
| SARGe | 5 | 1 | 200 | 1000 |

*Estimated Total Annual Burden Hours:* 1000.

**Additional Information**

Copies of the proposed collection may be obtained by writing to The Administration for Children and Families, Office of Information Services, 370 L'Enfant Promenade, SW., Washington, DC 20447, Attn: ACF Reports Clearance Officer.

**OMB Comment**

OMB is required to make a decision concerning the collection of information between 30 and 60 days after publication of this document in the **Federal Register.** Therefore, a comment is best assured of having its full effect if OMB receives it within 30 days of publication. Written comments and recommendations for the proposed information collection should be sent directly to the following: Office of Management and Budget, Paperwork Reduction Project, 725 17th Street, NW., Washington, DC 20503, Attn: Desk Officer for ACF.