of the estimated burden; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) the use of automated collection techniques or other forms of information technology to minimize the information collection burden.

Type of Information Collection Request: Revision of a Currently Approved Collection; *Title of Information Collection:* The National Data Reporting Requirements (NDRR). We are requesting the name of the collection be changed to the Fiscal Soundness Reporting Requirements (FSRR) and Supporting Regulations in 42 CFR 417., .126.478,. 162; *Form No.:* HCFA–906 (OMB# 0938–0469); *Use:* HCFA needs this information to establish an on-going fiscal soundness of the Managed Care Organizations in the Medicare + Choice Program; *Frequency:* Quarterly; *Affected Public:* Business or other for-profit; *Number of Respondents:* 300; *Total Annual Responses:* 300; *Total Annual Hours:* 301.

To obtain copies of the supporting statement for the proposed paperwork collections referenced above, access HCFA's WEB SITE ADDRESS at http://www.hcfa.gov/regs/prdact95.htm, or E-mail your request, including your address and phone number, to Paperwork@hcfa.gov, or call the Reports Clearance Office on (410) 786–1326. Written comments and recommendations for the proposed information collections must be mailed within 30 days of this notice directly to the OMB Desk Officer designated at the following address:OMB Human Resources and Housing Branch, Attention: Allison Eydt, New Executive Office Building, Room 10235, Washington, DC 20503.

Dated: September 27, 2001.

John P. Burke III,

CMS Reports Clearance Officer, CMS, Office of Information Services, Security and Standards Group, Division of CMS Enterprise Standards.

[FR Doc. 01–25545 Filed 10–10–01; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare and Medicaid Services

Privacy Act of 1974; Report of New System of Records

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare and 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 SOR titled, ''Provider Enrollment, Chain, and Ownership System (PECOS),'' HHS/CMS/OFM, System No. 09–70–0532. PECOS will be used to collect and maintain provider/supplier enrollment information from the Medicare Provider/Supplier Enrollment Application and related forms (Form(s) HCFA–855A, 855B, 855I, 855R, and, 855S). PECOS will collect information provided by the applicant related to identity, qualifications, practice locations, ownership, billing arrangements, reassignment of benefits, surety and bond data, clearinghouses submitting electronic claims, and related organizations. PECOS will also maintain information on business owners, chain home offices and provider/chain associations, managing/directing employees, partners, authorized and delegated representatives, supervising physicians of the supplier, staffing companies, ambulance crew members, and/or interpreting physicians and related technicians. Managing/directing employees include general managers, business managers, administrators, directors, and other individuals who exercise operational or management control over the provider/supplier.

The primary purpose of the SOR is to: (1) Collect information for an applying provider/supplier and record the associations between the applicant and those who have an ownership or control interest in the entity; (2) permit informed enrollment decisions to be made based on past and present business history, any reported exclusions, sanctions and felonious behavior at their location or in multiple contractor jurisdictions; and, (3) ensure that correct payments are made under the Medicare program. Information retrieved from this SOR will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent; (3) support constituent requests made to a congressional representative; (4) support litigation involving the Agency; and (5) combat fraud and abuse in certain health benefits 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 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 September 26, 2001. To ensure that all parties have adequate time in which to comment, the new SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution, CMS, Mailstop 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: Michael Collett, Health Insurance Specialist, Division of Provider/Supplier Enrollment, Program Integrity Group, Office of Financial Management, CMS, N3–10–07, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–6121.

SUPPLEMENTARY INFORMATION:

I. Description of the Proposed SOR

A. Background

Prior to PECOS, a national tracking mechanism has not been available to connect those who bill Medicare and those who receive Medicare monies, thus allowing potential fraud and abuse within the Medicare system. With information maintained in PECOS, it will now be possible to link providers/suppliers to the people and organizations with which they have a business relationship and to identify those involved in illegal Medicare activities. Additionally, PECOS will enumerate chain home offices and maintain provider/chain associations. Previously, Medicare contractors collected enrollment information on their own unique application forms. In

May 1996, CMS created the Form HCFA 855 and its iterations (855A for change of information, 855R for reassignment of benefits, and 855S for Durable Medial Equipment, Prosthetics, Orthotics, and Suppliers (DMEPOS) enrollment), in order to standardize the collection of the various types of provider/supplier data at the time of the provider/supplier's initial enrollment. Identifying data will be entered into the PECOS. PECOS will also retain the information on business owners, managing/directing employees, partners, authorizing representatives, and/or supervising physicians of the supplier. Managing/directing employees include general managers, business managers, administrators, directors, and other individuals who exercise operational or managerial control over the provider/supplier. With the information provided by the provider/supplier, Medicare contractors will be able to make informed enrollment decisions based on past and present business history as well as information regarding any exclusions, sanctions, and felonious behavior.

CMS is authorized to collect information on the Form HCFA 855 to ensure that correct payments are made to providers/suppliers under the Medicare program as established by Title XVIII of the Social Security Act, and, section 31001(I) of the Debt Collection Improvement Act (DCIA) of 1996 (Pub. L.104–134), as amended (Title 31 United States Code (USC) 7701), by adding paragraph (c) to require that any person or entity doing business with the Federal government must provide his or her tax identification number (TIN).

The Balanced Budget Act of 1997 (BBA) (Pub. L. 105–33), section 4313, requires disclosure of both the employer identification number (EIN) and the social security number (SSN) of each person with ownership or control interest in the provider/supplier and any subcontractor in which the entity directly or indirectly has a 5 percent or more ownership interest as well as any managing/directing employees. The ''Report to Congress on Steps Taken to Assure Confidentiality of Social Security Account Numbers as Required by the Balanced Budget Act,'' was signed by the Secretary and sent to Congress on January 26, 1999, with mandatory collection of SSNs and EINs effective on or about April 26, 1999.

The BBA also instructs CMS to transmit the EIN to the Department of Treasury and SSN to the SSA for verification. By collecting, verifying, and storing the SSN and EIN of these individuals, CMS contractors throughout the United States will have a coordinated national system and be able to view any enrollment form. Consistent application of Medicare rules for program enrollment, credentialing, and claims submission will aid in the identification of medical personnel, and those affiliated with them, who have been excluded by the Office of the Inspector General, cited on the General Services Administration's ''List of Excluded Parties'' found not compliant with Medicare rules and regulations, or have questionable business practices. All denials, revocations, and exclusions information will be maintained in PECOS.

B. Statutory and Regulatory Basis for SOR

Authority for maintenance of the system is given under sections 1102(a) (Title 42 U.S.C. 1302(a)), 1128 (42 U.S.C. 1320a–70), 1814(a) (42 U.S.C. 1395f(a)(1), 1815(a) (42 U.S.C. 1395g(a)), 1833(e) (42 U.S.C. 1395(e), 1871 (42 U.S.C. 1395hh), and 1886(d)(5)(F), (42 U.S.C. 1395ww(d)(5)(F) of the Social Security Act; 1842(r) (42 U.S.C. section 9202(g)); section 1124(a)(1) (42 U.S.C. 1320a–3(a)(1), and 1124A (42 U.S.C. 1320a–3a), section 4313, as amended, of the BBA of 1997; and section 31001(I) (31 U.S.C. 7701) of the DCIA (P.L. 104–134), as amended.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

PECOS will contain information on health care providers, provider of medical or other health services, Medicare facilities and practitioners, assorted clinics, physicians, clinical laboratories, suppliers of durable medical equipment, other licensed/certified health care practitioners, and any other person who furnishes health care services or supplies. This system will also contain information on certified, as well as uncertified provider/supplier entities and their owners, managing/directing employees, officials of the entity, chief executive officer, senior or majority partner, authorized or delegated representatives, and supervisory physicians of such supplier.

This SOR will contain the names, SSNs, and EINs for each disclosing entity and owners with 5 percent or more ownership or control interest, as well as managing/directing employees. Managing/directing employees include general manager, business managers, administrators, directors, and other individuals who exercise operational or managerial control over the provider/supplier. Additional information includes other identifiers, name(s), demographic data, educational/professional data, past and present business history, as well as questions regarding any exclusions, sanctions, and felonious behavior.

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

We are establishing the following policies, procedures, and restrictions on routine use disclosures of information that will be maintained in the system. In general, routine uses of this file (or a subset thereof) will be approved for the minimum set of data elements in the record needed to accomplish the purpose of the disclosure after CMS:

(a) Determines that the use or disclosure is consistent with the reason that the data are being collected: (1) Detecting and tracking fraudulent providers and suppliers; (2) establishing correct payments based on qualifications of providers and suppliers; and, (3) ensuring that the location where the service is rendered is appropriate.

(b) Determines:

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

(2) 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

(3) That there is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

(c) Requires the information recipient to:

(1) Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record; and

(2) Remove or destroy at the earliest time all provider/supplier identifiable information.

(d) Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

Entities That 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 PECOS 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 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 the following routine use disclosures of information maintained in the system:

1. To agency contractors, or consultants that have been contracted by the agency to assist in accomplishment of a CMS function relating to the purposes for this system of records 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 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 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 requiring the contractor or consultant to return or destroy all information at the completion of the contract.

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent 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 with other activities within the state.

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

We also contemplate disclosing information under this routine use in situations in which state certifying agencies require PECOS information to assist in accomplishing functions relating to purposes for this SOR.

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.

Beneficiaries, as well as other individuals, may 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,

(c) any employee of the Agency in his or her individual capacity where DOJ has agreed to represent the employee, or

(d) Where 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 FIs 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 PECOS information for the purpose of combating fraud and abuse in such Federally funded programs.

IV. Safeguards

The PECOS system will conform with 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 1974, 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 the 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 and systems security requirements. Employees and contractors that 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 work-station and the 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 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 is 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 PECOS 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 systems 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 includes:

- User Logons—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 Logout—Access to the NT workstation is automatically logged out after 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 for 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.

There are several levels of security found in the PECOS system. Windows NT provides much of the overall system security. The Windows NT security model is designed to meet the C2-level criteria as defined by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria document (DoD 5200.28–STD, December 1985). Netscape Enterprise Server is the security mechanism for all transmission connections to the system. As a result, Netscape controls all information access requests. Anti-virus software is applied at both the workstation and at NT server levels.

Access to different areas on the Windows NT server are maintained through the use of file, directory, and share level permissions. These different levels of access control provide security that is managed at the user and group level within the NT domain. The file and directory level access controls rely on the presence of an NT File System hard drive partition. This provides the most robust security and is tied directly to the file system. Windows NT security is applied at both the workstation and at NT server levels.

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. Effects of the Proposed System of Records 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 PECOS. Disclosure of information from the system of records 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 maintained in this system in an effort 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: September 24, 2001.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0532

SYSTEM NAME:

Provider Enrollment, Chain, and Ownership System (PECOS), 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:

PECOS will collect information provided by the applicant related to identity, qualifications, practice locations, ownership, billing arrangements, reassignment of benefits, surety and bond data, clearinghouses submitting electronic claims, and related organizations. PECOS will also maintain information on business

owners, chain home offices and provider/chain associations, managing/directing employees, partners, authorized and delegated representatives, supervising physicians of the supplier, staffing companies, ambulance crew members, and/or interpreting physicians and related technicians. Managing/directing employees include general managers, business managers, administrators, directors, and other individuals who exercise operational or managerial control over the provider/supplier.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system of records will contain the names, social security numbers (SSN), and employer identification numbers (EIN) for each disclosing entity, owners, as well as managing/directing employees, with 5 percent or more ownership or control interest. Managing/directing employees include general manager, business managers, administrators, directors, and other individuals who exercise operational or managerial control over the provider/supplier. The system will also contain the Unique Provider Identification Number, demographic data, professional data, past and present business history as well as information regarding any exclusions, sanctions, and felonious behavior.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under sections 1102(a) (Title 42 United States Code (U.S.C.) section 1302(a)), 1128 (42 U.S.C. 1320a–70), 1814(a) (U.S.C. 1395f(a)(1), 1815(a) (42 U.S.C. 1395g(a)), 1833(e) (42 U.S.C. 1395(e), 1871 (42 U.S.C. 1395hh), and 1886(d)(5)(F), (42 U.S.C. 1395ww(d)(5)(F) of the Social Security Act; 1842(r) (42 U.S.C. 9202(g)); sec. 1124(a)(1) (42 U.S.C. 1320a–3(a)(1), and section 1124A (42 U.S.C. 1320a–3a), 4313, as amended, of the Balanced Budget Act of 1997; and section 31001(I) (31 U.S.C. 7701) of the Debt Collection Improvement Act of 1996 (Pub. L. 104–134), as amended.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the SOR is to: (1) Collect information for an applying provider/supplier and record the associations between the applicant and those who have an ownership or control interest in the entity; (2) permit informed enrollment decisions to be made based on past and present business history, any reported exclusions, sanctions and felonious behavior at their location or in multiple contractor jurisdictions; and, (3) ensure that correct payments are made under the Medicare program. Information retrieved from this SOR will also be disclosed to: (1) support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent; (3) support constituent requests made to a congressional representative; (4) support litigation involving the Agency; and (5) combat fraud and abuse in certain health benefits 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 PECOS 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 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 the following routine use disclosures of information maintained in the system:

1. To agency contractors, or consultants that have been engaged by the agency to assist in accomplishment of a CMS function relating to the purposes for this system of records and who need to have access to the records in order to assist CMS.

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent 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 with other activities within the state.

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) An employee of the Agency in his or her official capacity,

(c) An employee of the Agency in his or her individual capacity where DOJ has agreed to represent the employee, or

(d) Where 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 FIs 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:

All records are stored on paper and magnetic media.

RETRIEVABILITY:

The records are retrieved by the Internal Provider Control Number, SSN, EIN, or other CMS assigned provider numbers.

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 PECOS 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. Systems 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:

CMS will retain identifiable data for a total period of 15 years from the date the information was collected.

SYSTEM MANAGERS AND ADDRESS:

Director, Division of Provider/Supplier Enrollment, Office of Financial Management, CMS, 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, SSN, EIN, and for verification purposes, the subject individual's name (woman's maiden name, if applicable).

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 system is received from the Form(s) HCFA 855A, ''Application for Health Care Providers that will Bill Medicare Fiscal Intermediaries, HCFA 855B, ''Application for Health Care Providers that will Bill Medicare Carriers,'' HCFA 855I, ''Application for Individual Health Care Practitioners,'' HCFA 855R, ''Application for Reassignment of Medicare Benefits,'' and HCFA 855S, ''Durable Medial Equipment, Prosthetics, Orthotics, and Suppliers Application.''

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 01–24439 Filed 10–10–01; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

Notice of Availability

SUMMARY: The Fish and Wildlife Service has published a Comprehensive Conservation Plan and a Finding of No Significant Impact for both Lower Suwannee and Cedar Keys National Wildlife Refuges. Lower Suwannee Refuge is located in Dixie and Levy Counties, Florida, and Cedar Keys Refuge is located in Levy County, Florida. These plans describe how the Fish and Wildlife Service will manage the refuges for the next 15 years.

ADDRESSES: Copies of the above documents may be obtained by writing to Kenneth Litzenberger, Refuge Manager, Lower Suwannee National Wildlife Refuge, 16450 NW 31st Place, Chiefland, Florida 32626–4874. Copies of both plans are also available at the following website address: http://lowersuwannee.fws.gov.

SUMMARY INFORMATION: The plans provide clear statements regarding management of the refuges; ensure that management of the refuges reflect policies and goals of the National Wildlife Refuge System; ensure that management is consistent with federal, state, and county plans; provide long-term continuity in refuge management; and provide a basis for operation, maintenance, and capital improvement budget requests. The Finding of No Significant Impact is in response to environmental documentation prepared subsequent to the National Environmental Policy Act, 1969, which requires the disclosure of environmental impacts of any major federal action significantly affecting the quality of the human environment.

Authority: This notice is published under the authority of the National Wildlife Refuge System Improvement Act of 1997, Public Law 105–57. Some of the major issues addressed in the plans include restoration and maintenance of health water regimes; reduce of exotic and invasion plants; expansion of wildlife species inventory and increased mapping of habitat; enhancement of wildlife habitat for migratory and resident songbirds; and expansion of wildlife-dependent and other compatible recreation opportunities.

Dated: September 19, 2001.

Sam D. Hamilton,

Regional Director.

[FR Doc. 01–25487 Filed 10–10–01; 8:45 am]

BILLING CODE 4310–55–M

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

Notice of Receipt of Applications for Permit

Endangered Species

The public is invited to comment on the following application(s) for a permit to conduct certain activities with endangered species. This notice is provided pursuant to section 10(c) of the Endangered Species Act of 1973, *as amended* (16 U.S.C. 1531, *et seq.*). Written data, comments, or requests for copies of these complete applications should be submitted to the Director (address below) and must be received within 30 days of the date of this notice.

Applicant: Hawthorn Corporation, Grayslake, IL, PRT–843875

The applicant requests the re-issuance of a permit to export, re-export and re-import tigers (*Panthera tigris*) and progeny of the animals currently held by the applicant and any animals acquired in the United States by the applicant to/from worldwide locations to enhance the survival of the species through conservation education. This notification covers activities conducted by the applicant over a three year period.

Applicant: Hawthorn Corporation, Grayslake, IL, PRT–047787

The applicant requests a permit to export, re-export and re-import tigers (*Panthera tigris*) and progeny of the animals currently held by the applicant and any animals acquired in the United States by the applicant to/from worldwide locations to enhance the survival of the species through