studies or other review activities, conducted pursuant to Part B of Title XI of the Act and in performing affirmative outreach activities to individuals for the purpose of establishing and maintaining their entitlement to Medicare benefits or health insurance plans.

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.

7. To a CMS contractor (including, but not limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

8. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

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

STORAGE:

Computer diskette and on magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by the name, SSN, and/or HICN of claimant.

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 RECON system. For computerized records, safeguards have been established in accordance with the Department of Health and Human Services (HHS) standards and National Institute of Standards and Technology guidelines, e.g., security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management Circular #10, Automated Information Systems Security Program; CMS Information Systems Security Policy, Standards, and Guidelines Handbook, and OMB Circular No. A–130, Appendix III.

RETENTION AND DISPOSAL:

Records are maintained in a secure storage area with identifiers. Case records are transferred to and maintained in an archival file for a period of 15 years.

SYSTEM MANAGER AND ADDRESS:

Director, Division of hearings, Appeals & Dispute Resolution, Center for Beneficiary Choices, CMS, 7500 Security Boulevard, Mailstop S1–05–06, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, HIC, address, date of birth, and sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and SSN. Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also 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:

Sources of information contained in this records system is obtained from the reconsideration requests made by or on behalf of Medicare beneficiaries and from inquiries from congressional offices, health plans, providers, state insurance commissioners, state regulators, disenrollment surveys, Medicare carriers or intermediaries, and QIO records.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–18167 Filed 7–22–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of Modified or Altered System

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

ACTION: Notice of modified or altered System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter an SOR, ''Medicare Supplier Identification File (MSIF), System No. 09–70–0530.'' We are deleting routine uses number 2 pertaining to a Medicaid state agency or its fiscal agent to assist in enforcing Medicare and Medicaid sanctions, and number 4 pertaining to contractors. Disclosures previously allowed by routine use number 2 pertaining to a Medicaid state agency will now be covered by proposed routine use number 5. Disclosures previously allowed by routine use number 4 pertaining to contractors will now be covered by proposed routine use

number 1. We propose to add routine use number 4 and 5 to combat fraud and abuse in certain health benefits 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' intention to disclose individual-specific information contained in this system. The routine uses will then be prioritized and reordered according to their proposed usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization and to update language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of this system is to identify supplier businesses that eligible to receive Medicare payments for items and services furnished to Medicare beneficiaries as well as owners, managing employees, and subcontractors in those suppliers. The system will facilitate the identification of business owners who have been sanctioned by the Office of Inspector General and/or have questionable business practices within the Medicare program. The carriers will be able to review questionable claims before payment that has been found to be more effective than post-payment reviews. Information retrieved from this SOR will also be disclosed to: support regulatory, reimbursement, 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, and 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 modified 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 June 24, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution (DDLD), CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.–3 p.m., eastern daylight time.

FOR FURTHER INFORMATION CONTACT: Charles Waldhauser, Project Officer, Program Integrity Group, Office of Financial Management, CMS, Mail stop N3–02–16, 7500 Security Boulevard, Baltimore, Maryland, 21244–1850. The telephone number is 410–786–6140.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Statutory and Regulatory Basis for SOR

In 1992, CMS established a SOR under the authority of sections 1124, 1124A, 1126, and 1833(e) of Title XVIII of the Social Security Act (the Act) (Title 42 United States Code (USC) §§ 405, 426, 1395c, and 1395k). Notice of this system, ''Medicare Supplier Identification File (MSIF), System No. 09–70–0530,'' was most recently published in the **Federal Register** (FR) 57 FR 23420 (June 3, 1992), one routine use was added at 61 FR 6645 (Feb. 21, 1996), three new fraud and abuse routine uses were added at 63 FR 38414 (July 16, 1998), and at FR 50552 (Aug. 18, 2000), two of the fraud and abuse routine uses were revised and a third deleted.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

This system contains information on owners and managing employees of suppliers of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS), ambulance companies, imaging technology companies, and independent diagnostic testing facilities which provide service or supplies to Medicare beneficiaries. A ''supplier'' of DMEPOS is an entity or individual, including a physician or Part A provider, that sells or rents Part B covered items to Medicare beneficiaries and that meets the standards which CMS has established and found in 42 CFR § 424.57.

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 MSIF information as provided for under ASection III. Proposed Routine Use Disclosures of Data in the System.≃

We will only collect the minimum personal data necessary to achieve the purpose of MSIF. 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 only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, e.g., identifying supplier businesses, owner, and managing employees of those suppliers who provide services to Medicare beneficiaries.

2. Determines that:

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

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

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

3. Requires the information recipient to:

a. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

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

c. Agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the MSIF 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 engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this SOR and who need to have access to the records in order to assist CMS.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing a CMS function relating to purposes for this SOR. CMS occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or consultant whatever information is necessary for the contractor or consultant to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or consultant from using or disclosing the information for any purpose other than that described in the contract and requires the contractor or consultant to return or destroy all information at the completion of the contract.

2. To 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 and other individuals often 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.

3. 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' 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.

4. 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 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.

5. 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 MSIF 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 (Dec. 28, 00), as amended by 66 FR 12434 (Feb. 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

Administrative Safeguards

The MSIF 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 1974, Computer Security Act of 1987, the Paperwork Reduction Act (PRA) 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 Office and Management and Budget (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 assure 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 (QI) 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 MSIF 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 grant 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 (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

• User Log-ons—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 SOR 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 MSIF. 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 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: June 24, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

No. 09–70–0530

SYSTEM NAME:

''Medicare Supplier Identification File (MSIF), HHS/CMS/OFM''

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data

SYSTEM LOCATION:

National Supplier Clearing House, Palmetto Government Benefits Administrators, Interstate-20 at Alpine Road, Columbia, South Carolina 29219.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system of records (SOR) will contain information on owners and managing employees of suppliers of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS), ambulance companies, imaging technology companies, and independent diagnostic testing facilities which provide service or supplies to Medicare beneficiaries. A ''supplier'' of DMEPOS is an entity or individual, including a physician or Part A provider, that sells or rents Part B covered items to Medicare beneficiaries and that meets the standards that CMS has established and found in 42 CFR 424.57.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains the business names and addresses, owner's name, owner's social security number, Unique Physician/Practitioner Identification Number (UPIN), managing employee's name, employer identification number or other tax reporting number, and the carrier assigned billing numbers.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of this SOR is given under the provisions of §§ 1124, 1124A, 1126, and 1833(e) of Title XVIII of the Social Security Act (Title 42 United States Code (USC) §§ 405, 426, 1395c, and 1395k).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of this system is to identify supplier businesses that are eligible to receive Medicare payments for items and services furnished to Medicare beneficiaries as well as owners, managing employees, and subcontractors in those suppliers. The system will facilitate the identification of business owners who have been sanctioned by the Office of Inspector General and/or have questionable business practices within the Medicare program. The carriers will be able to review questionable claims before payment that has been found to be more effective than post-payment reviews. Information retrieved from this SOR will also be disclosed to: support regulatory, reimbursement, 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, and 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:

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a ''routine use.'' The proposed routine use in this system meets the compatibility requirement of the Privacy Act. This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, 65 FR 82462 (Dec. 28, 00), as amended by 66 FR 12434 (Feb. 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 the following routine use disclosures of information that 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 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.

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

4. 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.

5. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

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

STORAGE:

Computer diskette and on magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by the business names and addresses, owner's name, owner's social security number, UPIN, managing employee's name, employer identification number or other tax reporting number, and the carrier assigned billing 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 MSIF system. For computerized records, safeguards have been established in accordance with the Department of Health and Human Services (HHS) standards and National Institute of Standards and Technology guidelines, e.g., security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management Circular #10, Automated Information Systems Security Program; CMS Automated Information Systems Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

RETENTION AND DISPOSAL:

Records are maintained in a secure storage area. Records are maintained by CMS and the repository of the National Archives and Records Administration for a period not to exceed 15 years.

SYSTEM MANAGER AND ADDRESS:

Director, Program Integrity Group, Office of Financial Management, CMS, C3–02–16, 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 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:

Sources of information contained in this records system include data collected from the application which the supplier completes to obtain Medicare billing numbers. (CMS Form 192-prior to August 1996, CMS Form 885, April 1996–May 1997, and CMS Form 855S-after May, 1997).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–18168 Filed 7–22–02; 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 (formerly the Health Care Financing Administration).

ACTION: Notice of modified or altered System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter an SOR, ''Intern and Resident Information System (IRIS), No. 09–70–0524.'' We will broaden the scope of this system to include information on interns and residents (IRs) required in Title 42 Code of Federal Regulations (CFR) § 412.105 (Special treatment: Hospitals that incur indirect costs for graduate medical education programs) and 42 CFR 413.86 (Direct graduate medical education payments). We are also deleting published routine use number 3 authorizing disclosures to contractors, number 6 authorizing disclosures to researchers, and an unnumbered routine use which authorizes the release of information to the Social Security Administration (SSA).

Proposed routine use number 1 will now cover disclosures previously allowed by routine use number 3 pertaining to contractors. Access to the data from this system to SSA will be accomplished by adding a new routine use number 4, which authorizes release of information in this system to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' Routine use number 6 authorizing release to researchers is being deleted because the very specific nature of the data collected is not sought for research purposes.

The security classification previously reported as ''None'' will be modified to reflect that the data in this system are considered to be ''Level Three Privacy Act Sensitive.'' We are modifying the language in the remaining routine uses to provide clarity to CMS's intention to disclose individual-specific information contained in this system. The routine uses will then be prioritized and reordered according to their proposed usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization and to update language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of the SOR is to ensure that no IRs are counted by the Medicare program as more than one full-time equivalent (FTE) employee in the calculation of payments for the costs of direct graduate medical education (GME) and indirect medical education (IME). Information retrieved from this SOR will also be disclosed to: support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant, providers and suppliers of services, third-party contacts where necessary to establish or verify information, another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, support constituent requests made to a congressional representative, support litigation involving the Agency, and 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 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 June 24, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution (DDLD), CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 am.–3 pm., Eastern daylight time.

FOR FURTHER INFORMATION CONTACT: Milton Jacobson, Division of Financial Integrity, Office of Financial Management, CMS, Room C3–14–00, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–7553.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Statutory and Regulatory Basis for the SOR

In 1990, CMS established a SOR under the authority of sections 1886(d)(5)(B) and 1886(h) of the Social Security Act (the Act) (42 U.S.C. 1395ww(d)(5)(B) and 1395ww(h)). Notice of this system, ''Intern and Resident Information System,'' System No. 09–70–0524, was published in the **Federal Register** (FR) at 55 FR 51163–51165 (Dec. 12, 1990). An unnumbered routine use was added for SSA at 61 FR 6645 (Feb. 21, 1996), three new fraud and abuse routine uses were added at 63