DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of a Modified or Altered System of Records

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS).

ACTION: Notice of a Modified or Altered System of Records (SOR).

SUMMARY: In accordance with the Privacy Act of 1974, we are proposing to modify or alter an existing SOR, ''Medicare Supplier Identification File (MSIF),'' System No. 09–70–0530, last published at 67 **Federal Register** 48184 (July 23, 2002). 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. We propose to modify existing routine use number 1 that permits disclosure to agency contractors and consultants to include disclosure to CMS grantees who perform a task for the agency. CMS grantees, charged with completing projects or activities that require CMS data to carry out that activity, are classified separate from CMS contractors and/or consultants. The modified routine use will remain as routine use number 1.

We will delete routine use number 2 authorizing disclosure to support constituent requests made to a congressional representative. If an authorization for the disclosure has been obtained from the data subject, then no routine use is needed. The Privacy Act allows for disclosures with the ''prior written consent'' of the data subject. We will broaden the scope of routine uses number 4 and 5, authorizing disclosures to combat fraud and abuse in the Medicare and Medicaid programs to include combating ''waste'' which refers to specific beneficiary/recipient practices that result in unnecessary cost to all Federally-funded health benefit programs.

We are modifying the language in the remaining routine uses to provide a proper explanation as to the need for the routine use and to provide clarity to CMS's intention to disclose individual-specific information contained in this system. The routine uses will then be prioritized and reordered according to their usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization or because of the impact of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Pub. L. 108–173) provisions and to update language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of this modified 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 information retrieved from this system of records will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant, or grantee; (2) support litigation involving the agency; and (3) combat fraud, waste, and abuse in Federally-funded 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 or altered routine uses, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

DATES: *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 Homeland Security & Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on November 28, 2006. To ensure that all parties have adequate time in which to comment, the modified system, including routine uses, will become effective 30 days from the publication of the notice, or 40 days from the date it was submitted to OMB and Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: CMS Privacy Officer, Division of Privacy Compliance, Enterprise Architecture and Strategy Group, Office of Information Services, 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: Barry Bromberg, Division of Provider/Supplier Enrollment, Program Integrity Group, Office of Financial Management, CMS, Mail Stop N3–02–16, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. He can also be reached by telephone at 410–786–9953, or via e-mail at *Barry.Bromberg@cms.hhs.gov.*

SUPPLEMENTARY INFORMATION: CMS established a new SOR, in 1992, 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 (U.S.C.) §§ 405, 426, 1395c, and 1395k). Notice of this system, MSIF, was most recently published in the **Federal Register** (Fed. Reg.) 67 FR 48184 (July 23, 2002), deleting 2 routine uses and updating the security classification, two fraud and abuse routine uses were revised and one deleted at 65 FR 50552 (August 18, 2000), one routine use was added at 61 FR 6645 (February 21, 1996), and at 57 FR 23420 (June 3, 1992).

I. Description of the Modified or Altered System of Records

A. Statutory and Regulatory Basis for SOR

Authority for maintenance of the system is given under sections 1124, 1124A, 1126, and 1833(e) of the Social Security Act (Title 42 United States Code (U.S.C.) §§ 1320a–3, 1320a–3a, 1320a–5, and 13951(e)).

B. Collection and Maintenance of Data in the System

MSIF contains information on owners and managing employees of suppliers of Durable Medicare Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS), which provide service or supplies to Medicare beneficiaries. The system contains, but is not limited to: Business names and addresses, owner's name, owner's social security number, Unique Physician/Practitioner Identification Number, managing employee's name, employer identification number or other tax reporting number, and the carrier assigned billing numbers.

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

A. 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 that can be associated with an individual as provided for under ''Section III. Proposed Routine Use Disclosures of Data in the System.'' Both identifiable and non-identifiable data may be disclosed under a routine use.

We will only 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. Disclosure of information from this system will be approved only to the extent necessary to accomplish the purpose of the disclosure and only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, *e.g.*, 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.

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. 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 uses in this system meet the compatibility requirement of the Privacy Act. We are proposing to establish the following routine use disclosures of information maintained in the system:

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

We contemplate disclosing this 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.

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

2. 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.

Whenever CMS is involved in litigation, and 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.

3. 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, waste, or abuse in such program.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual relationship or grant with a third party to assist in accomplishing CMS functions relating to the purpose of combating fraud, waste, and abuse.

CMS occasionally contracts out certain of its functions and makes grants 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.

4. 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, waste, 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, waste, or abuse in such programs.

Other agencies may require MSIF information for the purpose of combating fraud, waste, and abuse in such federally-funded programs.

B. Additional Provisions Affecting Routine Use Disclosures

To the extent this system contains Protected Health Information (PHI) as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, Subparts A and E) 65 FR 82462 (12–28–00). Disclosures of such PHI that are otherwise 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.'' (See 45 CFR 164–512(a)(1)).

In addition, our policy will be to prohibit release even of data not directly identifiable, except pursuant to one of the routine uses or if required by law, if we determine 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 an individual could, because of the small size, use this information to deduce the identity of the beneficiary).

IV. Safeguards

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: The Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

V. Effects of the Modified System of Records on Individual Rights

CMS proposes to modify 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 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 of patients whose data are 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 information relating to individuals.

Dated: November 24, 2006.

John R. Dyer,

Chief Operating Officer, Centers for Medicare & Medicaid Services.

SYSTEM 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:

MSIF contains information on owners and managing employees of suppliers of Durable Medicare Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS), which provide service or supplies to Medicare beneficiaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains, but is not limited to: business names and addresses, owner's name, owner's social security number (SSN), 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 the system is given under sections 1124, 1124A, 1126, and 1833(e) of the Social Security Act (Title 42, United States Code (U.S.C.) §§ 1320a–3, 1320a–3a, 1320a–5, and 13951(e)).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of this modified 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 information retrieved from this system of records will also be disclosed to: (1) support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant, or grantee; (2) support litigation involving the agency; and (3) combat fraud, waste, and abuse in Federally-funded health benefits programs.

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

B. 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 uses in this system meet the compatibility requirement of the Privacy Act. We are proposing to establish the following routine use disclosures of information maintained in the system:

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

2. 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.

3. 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, waste, or abuse in such program.

4. 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, waste, 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, waste, or abuse in such programs.

C. Additional Provisions Affecting Routine Use Disclosures:

To the extent this system contains Protected Health Information (PHI) as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, Subparts A and E) 65 FR 82462 (12–28–00). Disclosures of such PHI that are otherwise 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.'' (See 45 CFR 164–512(a)(1)).

In addition, our policy will be to prohibit release even of data not directly identifiable, except pursuant to one of the routine uses or if required by law, if we determine 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 an individual could, because of the small size, use this information to deduce the identity of the beneficiary).

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

STORAGE:

All records are stored on computer diskette and magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by the business names and addresses, owner's name, owner's SSN, UPIN, managing employee's name, employer identification number or other tax reporting number, and the Medicare contractor assigned billing numbers.

SAFEGUARDS:

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: all pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

RETENTION AND DISPOSAL:

Records are maintained by CMS for a period not to exceed 15 years. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Provider/Supplier Enrollment, Program Integrity Group, Office of Financial Management, CMS, Mail Stop 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, address, date of birth, and gender, 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 specify the record contents being sought. (These procedures are in accordance with department regulation 45 CFR 5b.5(a)(2).)

CONTESTING RECORDS PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the records 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.)

RECORDS 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 888—April 1996 through May 1997, and CMS Form 855S—after May 1997).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. E6–20409 Filed 12–1–06; 8:45 am]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Proposed Information Collection Activity; Comment Request

Proposed Projects:

Title: Form OCSE–396A: Financial Report;

Form OCSE–34A: Quarterly Report of Collections.

OMB No.: 0970–0181.

Description: State agencies administering the Child Support Enforcement Program under title IV–D of the Social Security Act are required to provide information each fiscal quarter to the Office of Child Support Enforcement (OCSE) concerning administrative expenditures and the receipt and disposition of child support payments from non-custodial parents. Together with a third quarterly report, ''Itemized Undistributed Collections'' (Schedule UDC—OMB No. 0970–0268), these forms provide information from each State that is used to compute the quarterly grant awards, the annual incentive payments and provide valuable information on program