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:

CMS will retain information for a total period not to exceed 5 years after the final report is released. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER AND ADDRESS:

Director Division of Institutional Post Acute Care, Chronic Care Policy Group, Center for Medicare Management, Mail Stop C5–06–27, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244–1849.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, employee identification number, tax identification number, national provider number, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), HICN, and/or 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).

RECORDS SOURCE CATEGORIES:

Data will be collected from OmniCare, pharmacies, nursing homes, and Long Term Care Minimum Data Set, System No. 09–70–1517.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. E6–18452 Filed 11–1–06; 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 New System of Records

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

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, CMS is proposing to establish a new system of records (SOR) titled ''One Program Integrity Data Repository (ODR),'' System No. 09–70–0568. Section 1893 of the Social Security Act (the Act) established the ''Medicare Integrity Program'' that requires CMS to contract with eligible entities to ''review activities of providers of services or other individuals and entities furnishing items and services for which payment may be made under this title'' by utilizing equipment and software technologies. Likewise, section 1893 of the Act requires CMS to establish the Medicare Medicaid Data Match Program (Medi-Medi) in which data from both the Medicare and Medicaid programs are analyzed together to better detect fraud, waste, and abuse existent in these programs. In order to comply with these requirements and enhance our ability to detect fraud, waste, and abuse in Medicare and Medicaid, CMS is proposing to construct the ODR.

CMS maintains numerous systems housing Medicare beneficiary Parts A, B, C, and D entitlement, enrollment, and utilization information. Additionally, CMS maintains data on physicians, providers, employer plans, Medicaid recipients and Medicare secondary payers. There are a large number of data sources, extraction tools, and access mechanisms. Users of the data often experience inconsistent, untimely, or duplicated information. The ODR will be an enterprise resource that will provide an integrated view of the data to all of CMS and its partners providing a single authoritative source of information and providing quality and timely data.

The ODR will provide an organized structure for reaching the data through a consistent application of access policies, processes and procedures, common services, governance, and framework. The ODR will integrate and load data from various CMS systems consisting of Medicare Parts A, B, C, and D, Medicaid and Retiree Drug Subsidy entitlement, enrollment and utilization data. The ODR will also contain demographic information on Medicaid beneficiaries, Medicare providers and physicians, and employer plans that are receiving a subsidy from CMS for providing creditable drug coverage to their retirees. It is through the integration of this Medicare data with other data; *e.g.*, historic data, Part A and Part B data, and Medicaid data sets provided by state agencies that CMS fraud, waste, and abuse, quality improvement, research, and other analytic activities are maximized.

The data collected and maintained in this system are retrieved from the following databases: Medicare Drug Data Processing System, System No. 09–70–0553 (70 FR 58436 (October 6, 2005)); Medicare Beneficiary Database, System No. 09–70–0536 (66 FR 63392 (December 6, 2001)); Medicare Advantage Prescription Drug System, System No. 09–70–4001 (70 FR 60530 (October 18, 2005)); Medicaid Statistical Information System, System No. 09–70–6001 (67 FR 48906 (July 26, 2002)); Retiree Drug Subsidy Program, System No. 09–70–0550 (70 FR 41035 (July 15, 2005)); Common Working File, System No. 09–70–0526 (67 FR 3210 (January 23, 2002)); National Claims History,

System No. 09–70–0005 (67 FR 57015 (September 6, 2002)); Enrollment Database, System No. 09–70–0502 (67 FR 3203 (January 23, 2002)); Carrier Medicare Claims Record, System No. 09–70–0501 (67 FR 54428 (August 22, 2002)); Intermediary Medicare Claims Record, System No. 09–70–0503 (67 FR 65982 (October 29, 2002)); Unique Physician/Provider Identification Number, System No. 09–70–0525, (69 FR 75316 (December 16, 2004)); Medicare Supplier Identification File, System No. 09–70–0530 (67 FR 48184 (July 23, 2002)); and the Medicaid data sets provided by participating state agencies.

The primary purpose of this system is to establish an enterprise resource that will provide a single source of information for all CMS fraud, waste, and abuse activities. 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) assist another Federal or State agency, agency of a state government, an agency established by state law, or its fiscal agent; (3) support Quality Improvement Organizations (QIO); (4) assist other insurers for processing individual insurance claims; (5) facilitate research on the quality and effectiveness of care provided, as well as payment related projects; (6) support litigation involving the agency; and (7) combat fraud, waste, and abuse in certain health benefits programs. We have provided background information about the new 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 routine uses, CMS invites comments on all portions of this notice. *See Effective Date* section for comment period.

DATES: *Effective Date:* CMS filed a new SOR 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 October 27, 2006. To ensure that all parties have adequate time in which to comment, the new system will become effective 30 days from the publication of the notice, or 40 days from the date it was submitted to OMB and the congress, whichever is later. We may defer implementation of this system or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

ADDRESSES: The public should address comments to the CMS Privacy Officer, Division of Privacy Compliance, Enterprise Architecture and Strategy Group, Office of Information Services, Mail Stop 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: Christa Robertson, Division of Analysis and Evaluation, Program Integrity Group, Office of Financial Management, CMS, Room N3–07–04, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. She can be reached by telephone at 410–786–6965 or via e-mail at *Christa.Robertson@cms.hhs.gov.*

SUPPLEMENTARY INFORMATION: The ODR will work in conjunction with the Integrated Data Repository system of records to support the One Program Integrity (PI) Group. While the IDR will initially focus on fee-for-service and some prescription drug data, the ODR will initially focus on supplementary data to support the new Medicare Prescription Drug program along with Medicaid data to support the Medi-Medi contractors. CMS has contracted with Medicare Drug Integrity Contractors (MEDICs). The MEDICs are required to perform a myriad of functions including: fraud, waste, and abuse detection; coordination with law enforcement; data analysis to identify fraud, waste, and abuse; fraud, waste, and abuse audits; other audits as required; anti-fraud Part D education and outreach; and the development of a Part D error rate. Due to the complexity of Part D data, to perform the above-mentioned functions, it is imperative that MEDICs have access to a wide variety of CMS data, including Parts A, B, C, D and Medicaid data.

The Office of Financial Management, Program Integrity Group serves as the point of contact for program integrity issues related to Medicare benefits. Major Program Integrity Group program initiatives include the Program Safeguard Contractor Program, Medical Review, Provider and Supplier Enrollment, MMA Integrity, and cross cutting issues between Medicare and Medicaid including the 'Medi-Medi' program. As part of its program integrity work, the Program Integrity Group works closely with law enforcement (*e.g.*, Federal Bureau of Investigation, Department of Justice, Office of Inspector General). For example, the Program Integrity Group, and its contractors, refer potential fraud cases and fulfill law enforcement's requests for data. All of these functions can be better served through a comprehensive set of common data structures and modern tools that encourage collaboration and innovation.

I. Description of the Proposed System of Records

A. Statutory and Regulatory Basis for System

Authority for maintenance of this system is given under section 1893 of the Social Security Act.

B. Collection and Maintenance of Data in the System

This system will maintain information on Medicare beneficiaries Parts A, B, C, and D and physicians, providers, employer plans, Medicaid recipients and Medicare secondary payers.

Information maintained in the system include, but are not limited to: standard data for identification such as health insurance claim number, social security number, gender, race/ethnicity, date of birth, geographic location, Medicare enrollment, entitlement, and utilization information, Medicaid enrollment, entitlement, and utilization information, MSP data necessary for appropriate Medicare claim payment, hospice election, MA plan elections and enrollment, End Stage Renal Disease (ESRD) entitlement, historic and current listing of residences, and Medicare eligibility and Managed Care institutional status.

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

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

We will only disclose the minimum personal data necessary to achieve the purpose of ODR. 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

system will be approved only for the minimum information 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 establish an enterprise resource that will provide a single source of information for all CMS fraud, waste, and abuse activities.

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 individually-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, consultants or grantees who have been engaged by the agency to assist in the performance of a service related to this system and who need to have access to the records in order to perform the activity.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing 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 contractors, consultants or grantees 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 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' proper payment of Medicare and Medicaid 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 Federal/state Medicaid programs within the State.

Other Federal or State agencies in their administration of a Federal health program may require ODR information in order to support evaluations and monitoring of Medicare and Medicaid claims information of beneficiaries, including proper reimbursement for services provided. In addition, other state agencies in their administration of a Federal health program may require ODR information for the purpose of determining, evaluating and/or assessing cost effectiveness, and/or the quality of health care services provided in the State.

Disclosure under this routine use shall be used by state Medicaid agencies pursuant to agreements with HHS for determining Medicaid and Medicare eligibility, for quality control studies, for determining eligibility of recipients of assistance under Titles IV, XVIII, and XIX of the Act, and for the administration of the Medicaid program. Data will be released to the state only on those individuals who are patients under the services of a Medicaid program within the state who are residents of that State.

3. To Quality Improvement Organizations (QIO) in connection with review of claims, or in connection with 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.

As established by the Part D Program, QIOs will conduct reviews of prescription drug events data, or in connection with studies or other review activities conducted pursuant to Part D of Title XVIII of the Act.

QIOs will work to implement quality improvement programs, provide consultation to CMS, MA–PD, PDPs, and state agencies, to assist CMS in prescription drug event assessments, and prepare summary information for release to CMS.

QIOs will work to implement quality improvement programs, provide consultation to CMS, its contractors, and to State agencies. QIOs will assist State agencies in related monitoring and enforcement efforts, assist CMS and intermediaries in program integrity assessment, and prepare summary information for release to CMS.

4. To insurance companies, underwriters, third party administrators (TPA), employers, self-insurers, group health plans, health maintenance organizations (HMO), health and welfare benefit funds, managed care organizations, other supplemental insurers, non-coordinating insurers, multiple employer trusts, other groups providing protection against medical expenses of their enrollees without the beneficiary's authorization, and any entity having knowledge of the occurrence of any event affecting: (a) An individual's right to any such benefit or payment, or (b) the initial right to any such benefit or payment, for the purpose of coordination of benefits with the Medicare program and implementation of the Medicare Secondary Payer (MSP) provision at 42 U.S.C. 1395y (b). Information to be disclosed shall be limited to Medicare utilization data necessary to perform that specific function. In order to receive the information, they must agree to:

a. Certify that the individual about whom the information is being provided is one of its insured or employees, or is insured and/or employed by another entity for whom they serve as a TPA;

b. Utilize the information solely for the purpose of processing the individual's insurance claims; and

c. Safeguard the confidentiality of the data and prevent unauthorized access.

Other insurers, HMO, and Health Care Prepayment Plans may require ODR information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided.

CMS, using its coordination of benefits contractor, allows this to happen by having payers that will be secondary to part D submit their enrollment data in exchange for enrollment data. The data shared is mainly enrollment information (date of enrollment).

5. To an individual or organization for a research project or in support of an evaluation project related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.

The ODR data will provide for research or in support of evaluation projects, a broader, longitudinal, national perspective of the status of Medicare and Medicaid beneficiaries. CMS anticipates that many researchers will have legitimate requests to use this data in projects that could ultimately improve the care provided to Medicare and Medicaid beneficiaries and the policy that governs the care.

6. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. any employee of the agency in his or her official capacity, or

c. any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. the United States Government is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and 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.

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

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, 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 ODR 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 individuals 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 excessive or 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 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. 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: October 24, 2006.

John R. Dyer,

Chief Operating Officer, Centers for Medicare & Medicaid Services.

System No. 09–70–0568

SYSTEM NAME:

''One Program Integrity Data Repository (ODR), HHS/CMS/OFM''.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

The Centers for Medicare & Medicaid Services (CMS) Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system will maintain information on Medicare beneficiaries Parts A, B, C, and D and physicians, providers, employer plans, Medicaid recipients and Medicare secondary payers.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information maintained in the system include, but are not limited to: Standard data for identification such as health insurance claim number, social security number, gender, race/ethnicity, date of birth, geographic location, Medicare enrollment, entitlement, and utilization information, Medicaid enrollment, entitlement, and utilization information, MSP data necessary for appropriate Medicare claim payment, hospice election, MA plan elections and enrollment, End Stage Renal Disease (ESRD) entitlement, historic and current listing of residences, and Medicare eligibility and Managed Care institutional status.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of this system is given under section 1893 of the Social Security Act.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of this system is to establish an enterprise resource that will provide a single source of information for all CMS fraud and abuse activities. 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) assist another Federal or State agency, agency of a State government, an agency established by State law, or its fiscal agent; (3) support Quality Improvement Organizations (QIO); (4) assist other insurers for processing individual insurance claims; (5) facilitate research on the quality and effectiveness of care provided, as well as payment related projects; (6) support litigation involving the agency; and (7) combat fraud, waste, 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:

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, consultants or grantees who have been engaged by the agency to assist in the performance of a service related to this system and who need to have access to the records in order to perform the activity.

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' proper payment of Medicare and Medicaid 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 Federal/State Medicaid programs within the State.

3. To Quality Improvement Organizations (QIO) in connection with review of claims, or in connection with 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.

4. To insurance companies, underwriters, third party administrators (TPA), employers, self-insurers, group health plans, health maintenance organizations (HMO), health and welfare benefit funds, managed care organizations, other supplemental insurers, non-coordinating insurers, multiple employer trusts, other groups providing protection against medical expenses of their enrollees without the beneficiary's authorization, and any entity having knowledge of the occurrence of any event affecting: (a) An individual's right to any such benefit or payment, or (b) the initial right to any such benefit or payment, for the purpose of coordination of benefits with the Medicare program and implementation of the Medicare Secondary Payer (MSP) provision at 42 U.S.C. 1395y (b). Information to be disclosed shall be limited to Medicare utilization data necessary to perform that specific function. In order to receive the information, they must agree to:

a. Certify that the individual about whom the information is being provided is one of its insured or employees, or is insured and/or employed by another entity for whom they serve as a TPA;

b. Utilize the information solely for the purpose of processing the individual's insurance claims; and

c. Safeguard the confidentiality of the data and prevent unauthorized access.

5. To an individual or organization for a research project or in support of an evaluation project related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.

6. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. Any employee of the agency in his or her official capacity, or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. The United States Government is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and 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.

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

remedy, or otherwise combat fraud, waste, 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, 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.

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 individuals 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 electronically.

RETRIEVABILITY:

All records are accessible by HICN, SSN, and unique provider identification number.

SAFEGUARDS:

CMS has safeguards in place 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 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 will be retained until an approved disposition authority is obtained from the National Archives and Records Administration. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER AND ADDRESS:

Director, Division of MMA Integrity, Program Integrity Group, Office of Financial Management, CMS, Mailstop: 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, HICN, 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:

The data contained in this system of records are extracted from other CMS systems of records: Medicare Drug Data Processing System; Medicare Beneficiary Database; Medicare Advantage Prescription Drug System; State Medicaid Records; Medicaid Statistical Information System; Retiree Drug Subsidy Program; Common Working File; National Claims History; Enrollment Database; Carrier Medicare Claims Record; Intermediary Medicare Claims Record; Unique Physician/Provider Identification Number; Provider Enrollment Chain & Ownership System (PECOS); and Medicare Supplier Identification File. Information will also be provided from the participating state Medicaid agencies.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. E6–18454 Filed 11–1–06; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 2006N–0431]

Agency Information Collection Activities; Proposed Collection; Comment Request; Substantial Evidence of Effectiveness of New Animal Drugs

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA) is announcing an opportunity for public comment on the proposed collection of certain information by the agency. Under the Paperwork Reduction Act of 1995 (the PRA), Federal agencies are required to publish notice in the **Federal Register** concerning each proposed collection of information, including each proposed extension of an existing collection of information, and to allow 60 days for public comment in response to the