Medicare & Medicaid Services (CMS) (formerly the Health Care Financing Administration).

ACTION: Notice to delete 12 systems of records.

SUMMARY: CMS proposes to delete 12 systems of records from its inventory subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

EFFECTIVE DATE: The deletions will be effective on January 15, 2002.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution, CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is (410) 786–3573. 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 standard time.

SUPPLEMENTARY INFORMATION: CMS is reorganizing its databases because of the amount of information it collects to administer the Medicare and Medicaid programs. With this reorganization of databases, CMS is deleting the systems of records listed below. Retention and destruction of the data contained in these systems will follow the schedules listed in the system notice. CMS proposes to delete the following systems.

Systems to be Deleted:

System No. 09–70–0504, ''Beneficiary Part A and B Uncollectible Overpayment File;''
System No. 09–70–0508, ''Reconsideration and Hearing Cases Files (Part A) Hospital Insurance Program;''
System No. 09–70–0512, ''Review and Fair Hearing Case Files—Supplementary Medical Insurance Program;''
System No. 09–70–0516, ''Medicare Physician Supplier Master File;''
System No. 09–70–0518, ''Medicare Clinic Physician Supplier Master File;''
System No. 09–70–0522, ''Billing and Collection Master Record System;''
System No. 09–70–1511, ''Physical Therapists in Independent Practice (Individuals);''
System No. 09–70–1512, ''Peer Review Organizations Data Management Information System;''
System No. 09–70–1516, ''Uniform Clinical Data Set;''
System No. 09–70–2003, ''Completion of State Medicaid Quality Control Reviews;''
System No. 09–70–2006, ''Income and Eligibility Verification for Medicaid Eligibility Quality Control Reviews;''
System No. 09–70–9001, ''Health Care Financing Administration Correspondence and Assignment Tracking and Control System;''

Dated: January 14, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

[FR Doc. 02–1525 Filed 1–22–02; 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: Centers for Medicare & Medicaid Services (CMS) (formerly the Health Care Financing Administration), Department of Health and Human Services (HHS).

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

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, CMS is proposing to modify or alter an SOR, ''Health Insurance Master Record (HIMR),'' System No. 09–70–0502. CMS is reorganizing its databases because of the amount of information it collects to administer the Medicare program. We are proposing to amend the purpose of the HIMR to include maintaining enrollment data without utilization data and change the name from the HIMR to read the ''Enrollment Database (EDB)'' to reflect this amended purpose. The only data in the HIMR, which are not in the EDB, are the utilization and bill processing data. Since the EDB will now maintain enrollment-related data, all utilization data for bill payment record processing will now be maintained in the ''Common Working File (CWF),'' System No. 09–70–0526. With this reorganization of databases, CMS is deleting, in a separate notice, the following SOR: ''Medicare Enrollment Records Statistics (MERS),'' System No. 09–70–0006, and the ''Health Insurance Enrollment Statistics, General Enrollment Period (HIES),'' System No. 09–70–0007. These 2 systems are being deleted because their enrollment purpose is being subsumed into the EDB. The EDB does maintain data regarding direct billing for Medicare premiums.

The security classification previously reported as ''None'' will be modified to reflect that data in this system are considered to be ''Level Three Privacy Act Sensitive.'' We propose to delete published routine uses number 1 authorizing disclosures to the Railroad Retirement Board (RRB), number 2 authorizing disclosures to state welfare departments, number 3 authorizing disclosures to state audit agencies, number 8 authorizing disclosure to contractors, number 9 authorizing disclosures to state welfare agencies, number 12 authorizing disclosures to contractors, number 13 authorizing disclosures to agencies of a state government, number 14 authorizing disclosures to group health plans, number 15 authorizing disclosures to contractors, number 16 authorizing disclosures for Medicare Secondary Payer (MSP) utilization purposes, number 17 authorizing disclosures to the Internal Revenue Service (IRS), and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA).

Disclosures allowed by routine uses number 1, 2, 3, 13, 17, and to the SSA will be covered by a new routine use to permit release of information to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' The proposed routine use for contractors and consultants makes material changes to published routine uses number 8, 12, and 15, and as proposed should be treated as a new routine use. The proposed routine use for ''other insurers and group health plans'' makes material changes to published routine uses number 11, and 14, and as proposed should be treated as a new routine use. Routine use number 9 is being deleted because the information pertaining to Beneficiary State File and Carrier Alphabetical State File, is no longer maintained in the EDB. Routine use number 16 is also being deleted because the information listed in the routine use as being releasable for MSP utilization purposes is not maintained in the EDB.

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 usage. We will also take this opportunity to update any sections of this SOR that were affected by the recent reorganization and to modify language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of the SOR is to maintain information on Medicare enrollment for the administration of the Medicare program, including the following functions: ensuring proper Medicare enrollment, claims payment,

Medicare premium billing and collection, coordination of benefits by validating and verifying the enrollment status of beneficiaries, and validating and studying the characteristics of persons enrolled in the Medicare program including their requirements for information. Information retrieved from this SOR will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent; (3) providers and suppliers of services for administration of Title XVIII of the Act; (4) third parties where the contact is expected to have information relating to the individual's capacity to manage his or her own affairs; (5) Peer Review Organizations; (6) other insurers for processing individual insurance claims; (7) facilitate research on the quality and effectiveness of care provided, as well as payment-related and epidemiological projects; (8) support constituent requests made to a congressional representative; (9) support litigation involving the Agency; and (10) 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 SOR 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 January 15, 2002. We will not disclose any information under a routine use until 30 days after publication. We may defer implementation of this SOR or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution, CMS, 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: Bob Donnelly, Director, Health Plan Policy Group, Center for Beneficiary Choices, CMS, 7500 Security Boulevard, Mail Stop C4–25–02, Baltimore, Maryland 21244–1850. The telephone number is (410) 786–0629.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Background

The HIMR, which will be renamed the EDB, was established in 1965 to maintain accurate and complete data on Medicare enrollment, entitlement, and utilization. Notice of the modification to this system, HIMR, was published in the **Federal Register** (FR) at 55 FR 37549, (Dec. 18, 1990); 61 FR 6645 (Feb. 21, 1996) (added unnumbered social security use); 63 FR 38414 (July 16, 1998) (added three fraud and abuse uses); and 65 FR 50552 (Aug. 18, 2000) (deleted one and modified two fraud and abuse uses). MERS, was established to study the characteristics of persons enrolled in the Medicare program and establish the basis for Medicare services utilization rates. MERS is being deleted and the EDB will take over its enrollment purpose. HIES, was established to contact persons eligible for Part B benefits who had refused or withdrawn coverage of these benefits, for purposes of re-enrollment for Part B coverage and to evaluate results of such contacts. This system is also being deleted, and its enrollment purpose is being subsumed by the EDB. Utilization data from both will continue to be maintained in the CWF.

Since these systems were established, the amount of enrollment information CMS collects to administer the Medicare program has vastly increased. To be of maximum use, the data must be organized and categorized into a comprehensive system. This redesign of CMS's databases will result in changes to the collection, aggregation, and analysis of Medicare information. Changes in the way CMS processes its enrollment data are being dramatically affected by the database redesign activity. These changes are necessary to accomplish two major initiatives:

- Enrollment-related data will be processed at the CMS Data Center and not at the SSA National Computer Center;
- Enrollment-related data will be consolidated in one file from various sources.

The EDB is being created to serve as a shared data resource by all CMS information systems. Once the EDB is established, it will be the authoritative source of Medicare enrollment related information. It will identify, in the same manner as the HIMR did, each person currently or previously entitled to Medicare benefits based upon age, disability, or end-stage Renal Disease (ESRD) under Title XVIII of the Act or under provisions of the Railroad Retirement Act, and will also identify whether a person is currently covered or was previously covered for hospital insurance benefits (Part A), medical insurance benefits (Part B), or both.

Given these changes, the purpose statement of the EDB system must be amended to reflect its current function of maintaining enrollment data without utilization data. The amended purpose of the EDB will read as follows: ''To maintain information on Medicare enrollment for the administration of the Medicare program, including the following functions: ensuring proper Medicare enrollment, claims payment, Medicare premium billing and collection, coordination of benefits by validating and verifying the enrollment status of beneficiaries, and validating and studying the characteristics of persons enrolled in the Medicare program.''

B. Statutory and Regulatory Basis for SOR

Authority for maintenance of the system is given under sections 226, 226A, 1811, 1818, 1818A, 1831, 1836, 1837, 1838, 1843, 1876, and 1881 of the Social Security Act (the Act) and Title 42 Code of Federal Regulations (CFR), parts 406, 407, 408, 411 and 424.

Authority for maintenance of the system section 1862 of the Act was a published authority in the published SOR. We included section 1862 in the modified SOR since we do maintain a limited number of data elements in the EDB pertaining to MSP.

Authority for maintenance of the system section 1870 of the Act was included in the modified system since the EDB does maintain data regarding direct billing for Medicare premiums. Section 1870 (g) describes refunding these premiums.

II. Collection and Maintenance of Date in the System

A. Scope of the Data Collected

The system contains information related to Medicare enrollment and entitlement and MSP data containing other party liability insurance information necessary for appropriate Medicare claim payment. It contains hospice election, premium billing and collection, direct billing information, and group health plan enrollment data. The system also contains the

individual's health insurance numbers, name, geographic location, race/ethnicity, sex, and date of birth.

Information is collected on individuals age 65 or over who have been, or currently are, entitled to health insurance (Medicare) benefits under Title XVIII of the Act or under provisions of the Railroad Retirement Act, individuals under age 65 who have been, or currently are, entitled to such benefits on the basis of having been entitled for not less than 24 months to disability benefits under Title II of the Act or under the Railroad Retirement Act, individuals who have been, or currently are, entitled to such benefits because they have ESRD, individuals age 64 and 8 months or over who are likely to become entitled to health insurance (Medicare) benefits upon attaining age 65, and individuals under age 65 who have at least 21 months of disability benefits who are likely to become entitled to Medicare upon the 25th month of their being disabled.

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 EDB 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 EDB. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from the SOR 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 data is being collected; e.g., ensuring proper enrollment, establishing the validity of individual's entitlement to benefits, verifying the accuracy of information presented by the individual, insuring proper reimbursement for services provided, claims payment, and coordination of benefits provided to patients.

2. Determines that:

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

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

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

3. Requires the information recipient to:

a. Establish administrative, technical, and physical safeguards to prevent 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 EDB 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 or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, or consultants who have been contracted by the Agency to assist in 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 another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to:

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

b. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds, and/or

c. Assist Federal/state Medicaid programs within the state.

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

The IRS may require EDB data for the application of tax penalties against employers and employee organizations that contribute to Employer Group Health Plan or Large Group Health Plans that are not in compliance with 42 U.S.C.1395y(b);

In addition, other state agencies in their administration of a Federal health program may require EDB information for the purposes of determining, evaluating and/or assessing cost, effectiveness, and /or the quality of health care services provided in the state;

The RRB requires EDB information to administer provisions of the Railroad Retirement Act relating to railroad employment and/or the administration of the Medicare program;

SSA requires EDB data to assist in the implementation and maintenance of the Medicare program;

Disclosure under this routine use shall be used by state Medicaid agencies pursuant to agreements with the 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 or who are residents of that state;

We also contemplate disclosing information under this routine use in situations in which state auditing agencies require EDB information for auditing state Medicaid eligibility considerations. CMS may enter into an agreement with state auditing agencies to assist in accomplishing functions relating to purposes for this SOR.

3. To providers and suppliers of services directly or through fiscal intermediaries (FIs) or carriers for the administration of Title XVIII of the Act.

Providers and suppliers of services require EDB information in order to establish the validity of evidence or to verify the accuracy of information presented by the individual, as it concerns the individual's entitlement to benefits under the Medicare program, including proper reimbursement for services provided.

4. To third party contacts in situations where the party to be contacted has, or is expected to have information relating to the individual's capacity to manage his or her affairs or to his or her eligibility for, or an entitlement to, benefits under the Medicare program and,

a. The individual is unable to provide the information being sought (an individual is considered to be unable to provide certain types of information when any of the following conditions exists: the individual is confined to a mental institution, a court of competent jurisdiction has appointed a guardian to manage the affairs of that individual, a court of competent jurisdiction has declared the individual to be mentally incompetent, or the individual's attending physician has certified that the individual is not sufficiently mentally competent to manage his or her own affairs or to provide the information being sought, the individual cannot read or write, cannot afford the cost of obtaining the information, a language barrier exist, or the custodian of the information will not, as a matter of policy, provide it to the individual), or

b. The data are needed to establish the validity of evidence or to verify the accuracy of information presented by the individual, and it concerns one or more of the following: the individual's entitlement to benefits under the Medicare program, the amount of reimbursement, and in cases in which the evidence is being reviewed as a result of suspected fraud and abuse, program integrity, quality appraisal, or evaluation and measurement of activities.

Third parties contacts require EDB information in order to provide support for the individual's entitlement to benefits under the Medicare program; to establish the validity of evidence or to verify the accuracy of information presented by the individual, and assist in the monitoring of Medicare claims information of beneficiaries, including proper reimbursement of services provided.

5. To Peer Review Organizations (PROs) 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.

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

6. To insurance companies, third party administrators (TPA), employers, self-insurers, managed care organizations, other supplemental insurers, non-coordinating insurers, multiple employer trusts, group health plans (i.e., health maintenance organizations (HMOs) or a competitive medical plan (CMP) with a Medicare contract, or a Medicare-approved health care prepayment plan (HCPP)), directly or through a contractor, and other groups providing protection for their enrollees. Information to be disclosed shall be limited to Medicare entitlement data. 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 identified individual's insurance claims; and

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

Other insurers, TPAs, HMOs, and HCPPs may require EDB information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided.

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

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

8. To a Member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

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

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

a. The Agency or any component thereof, or

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

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

d. The United States Government,

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

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court, or adjudicatory body involved.

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

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.

11. 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 EDB information for the purpose of combating fraud and abuse in such Federally funded programs. Additional Circumstances Affecting Routine Use Disclosure

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 (12–28–00), as amended by 66 FR 12434 (2–26–01)). 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

A. Administrative Safeguards

The EDB system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1984, Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Office and Management and Budget (OMB) Circular A–130, Appendix III, ''Security of Federal Automated Information Resources.'' CMS has prepared a comprehensive system security plan as required by OMB Circular A–130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems. Paragraphs A–C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

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 insure security of the data, the proper level of class user is assigned for each individual user as determined at the Agency level. This prevents unauthorized users from accessing and modifying critical data. The system database configuration includes five classes of database users:

- Database Administrator class owns the database objects; *e.g.,* tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- Quality Indicator Report Generator class has read-only access to all fields and tables;
- Policy Research class has query access to tables, but 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 EDB 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 grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information System resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log on—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 System on Individual Rights

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. We will only disclose the minimum personal data necessary to achieve the purpose of EDB. 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 in this system 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: January 14, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0502

SYSTEM NAME:

Enrollment Database (EDB), HHS/CMS/CBC.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals age 65 or over who have been, or currently are, entitled to health insurance (Medicare) benefits under Title XVIII of the Act or under provisions of the Railroad Retirement Act; individuals under age 65 who have been, or currently are, entitled to such benefits on the basis of having been entitled for not less than 24 months to disability benefits under Title II of the Act or under the Railroad Retirement Act; individuals who have been, or currently are, entitled to such benefits because they have ESRD; individuals age 64 and 8 months or over who are likely to become entitled to health insurance (Medicare) benefits upon attaining age 65, and individuals under age 65 who have at least 21 months of disability benefits who are likely to become entitled to Medicare upon the 25th month of their being disabled.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information related to Medicare enrollment and entitlement and MSP data containing other party liability insurance information necessary for appropriate Medicare claim payment. It contains hospice election, Group Health Organization Insurance health plan election, premium billing and collection, direct billing information, and group health plan enrollment data. The system also contains the individual's health insurance numbers, name, geographic location, race/ethnicity, sex, and date of birth.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under sections 226, 226A, 1811, 1818, 1818A, 1831, 1836, 1837, 1838, 1843, 1876, and 1881 of the Act and Title 42 Code of Federal Regulations (CFR), parts 406, 407, 408, 411 and 424.

Authority for maintenance of the system section 1862 of the Act was a published authority in the published SOR. We included section 1862 in the modified SOR since we do maintain a limited number of data elements in the EDB pertaining to MSP.

Authority for maintenance of the system section 1870 of the Act was included in the modified system since the EDB does maintain data regarding direct billing for Medicare premiums. Section 1870 (g) describes refunding these premiums.

PURPOSE(S):

The primary purpose of the SOR is to maintain information on Medicare enrollment for the administration of the Medicare program, including the following functions: ensuring proper Medicare enrollment, claims payment, Medicare premium billing and collection, coordination of benefits by validating and verifying the enrollment status of beneficiaries, and validating and studying the characteristics of persons enrolled in the Medicare program including their requirements for information. Information retrieved from this SOR will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent; (3) providers and suppliers of services for administration of Title XVIII of the Act; (4) third parties where the contact is expected to have information relating to the individuals capacity to manage his or her own affairs; (5) Peer Review Organizations; (6) other insurers for processing individual insurance claims; (7) facilitate research on the quality and effectiveness of care provided, as well as payment-related and epidemiological projects; (8) support constituent requests made to a congressional representative; (9) support litigation involving the Agency; and (10) combat fraud and abuse in certain health benefits programs.

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

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the EDB without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

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 (12–28–00), as amended by 66 FR 12434 (2–26–01)). 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.'' We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, or consultants who have been contracted by the Agency to assist in 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 another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to:

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

b. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds, and/or

c. Assist Federal/state Medicaid programs within the state.

3. To providers and suppliers of services directly or through fiscal intermediaries (FIs) or carriers for the administration of Title XVIII of the Act.

4. To third party contacts in situations where the party to be contacted has, or is expected to have information relating to the individual's capacity to manage his or her affairs or to his or her eligibility for, or an entitlement to, benefits under the Medicare program and,

a. The individual is unable to provide the information being sought (an individual is considered to be unable to provide certain types of information when any of the following conditions exists: the individual is confined to a mental institution, a court of competent jurisdiction has appointed a guardian to manage the affairs of that individual, a court of competent jurisdiction has declared the individual to be mentally incompetent, or the individual's attending physician has certified that the individual is not sufficiently mentally competent to manage his or her own affairs or to provide the information being sought, the individual cannot read or write, cannot afford the cost of obtaining the information, a language barrier exist, or the custodian of the information will not, as a matter of policy, provide it to the individual), or

b. The data are needed to establish the validity of evidence or to verify the accuracy of information presented by the individual, and it concerns one or more of the following: the individual's entitlement to benefits under the Medicare program, the amount of reimbursement, and in cases in which the evidence is being reviewed as a result of suspected fraud and abuse, program integrity, quality appraisal, or evaluation and measurement of activities.

5. To Peer Review Organizations (PRO) 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.

6. To insurance companies, third party administrators, (TPA), employers, self-insurers, managed care organizations, other supplemental insurers, non-coordinating insurers, multiple employer trusts, group health plans (*i.e.,* health maintenance organizations (HMO) or a competitive medical plan (CMP) with a Medicare contract, or a Medicare-approved health care prepayment plan (HCPP)), directly or through a contractor, and other groups providing protection for their enrollees. Information to be disclosed shall be limited to Medicare entitlement data. 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 identified individual's insurance claims; and

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

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

8. 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.

9. 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.

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

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

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

STORAGE:

All records are stored on magnetic media.

RETRIEVABILITY:

All Medicare records are accessible by HIC number or alpha (name) search. This system supports both on-line and batch access.

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 EDB 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 (IRM) Circular #10, Automated Information Systems Security Program; CMS Automated Information Systems (AIS) Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

RETENTION AND DISPOSAL:

Records are maintained for a period of 15 years.

SYSTEM MANAGERS AND ADDRESS:

Director, Health Plan Policy Group, Center for Beneficiary Choices, CMS, 7500 Security Boulevard, 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, health insurance claim number, address, date of birth, and sex, 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 systems manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with department regulation 45 CFR 5b.7).

RECORD SOURCE CATEGORIES:

The data contained in these records are furnished by the individual, or in the case of some MSP situations, through third party contacts. There are cases, however, in which the identifying information is provided to the physician by the individual; the physician then adds the medical information and submits the bill to the carrier for payment. Updating information is also obtained from the Railroad Retirement Board, and the Master Beneficiary Record maintained by the SSA.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–1526 Filed 1–22–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare and Medicaid Services

Privacy Act of 1974; Report of 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 a system of records, ''Common Working File (CWF),'' System No. 09–70–0526. We propose to delete published routine uses number 1 authorizing disclosure to claimants and their authorized representatives, number 3 authorizing disclosure to third party contacts to establish or verify information, number 4 authorizing disclosure to the Treasury Department for investigating alleged theft, number 5 authorizing disclosure to the United States Postal Service (USPS), number 6 authorizing disclosure to the Department of Justice (DOJ) to combat fraud and abuse, number 7 authorizing disclosure to the Railroad Retirement Board (RRB), number 9 authorizing disclosure to State Licensing Board for review of unethical practices, number 12 authorizing disclosure to state welfare departments, number 14 authorizing disclosure to state audit agencies, number 16 authorizing disclosure to peer review groups to assist with questions of medical necessity, number 17 authorizing disclosure to physicians and other supplier of services attempting to validate amounts of individual items, number 18 authorizing disclosure to senior citizen volunteers to assist beneficiaries, number 19 authorizing disclosure to a contractor to recover erroneous Medicare payments, number 20 authorizing disclosure to state and other governmental Workers' Compensation Agencies, number 23 authorizing disclosure to an agency of a state government or established by law, and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA).

Disclosures permitted under routine uses number 4, 5, 7, 9, 12, 14, 20, 23, and to the SSA will be made a part of proposed routine use number 2. Proposed routine use number 2 will allow for release of information to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' Disclosures permitted under published routine uses number 1, 2, 3, and 18 will now be covered by proposed routine use number 3, which will allow for release of information to ''third party contacts.'' Disclosure to ''other insurers and group health plans'' contained in published routine use 21 has been broaden to include similar groups with similar activities. This routine use will be renumbered as proposed routine use number 6. Disclosures permitted under routine use number 6 will be covered by proposed routine use number 11, which will permit the release of data to other Federal agencies for the purposes of combating fraud and abuse. Disclosures permitted under routine use number 10 will be made a part of proposed routine use number 4, which will permit the release of data to physicians and providers of services. Routine use number 16 is being deleted because the information listed in the routine use as being releasable ''at the request of the carrier to assist in the resolution of questions of medical necessity, utilization and overutilization,'' is no longer maintained in the CWF. Routine use number 17 is also being deleted because the activity listed in the routine use unnecessarily duplicates activities described in proposed routine use number 4. Disclosures permitted under routine use number 19 will now be covered by proposed routine use number 10, which will permit the release of data to a CMS contractor or grantee for the purposes of combating fraud and abuse. We propose to renumber published routine use number 22 as proposed routine use number 1 and modify the language to clarify the circumstances for disclosure to contractors and consultants. We will establish a new proposed routine use number 9 to allow disclosure to DOJ for the purpose of representing Agency employees involved in litigation.

The security classification previously reported as ''None'' will be modified to