DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of Modified or Altered System

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) (formerly known as 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, CMS is proposing to modify or alter an SOR, ''National Claims History (NCH),'' System No. 09–70–0005. We propose to modify the purpose of this system by deleting from the NCH, a sub-file titled ''Expanded Modified Medicare Provider Analysis and Review File.'' This sub-file is used for statistical analyses bearing on Medicare payment policies for inpatient hospital services and skilled nursing facilities. To accomplish this activity, we propose to establish in a separate notice, a new SOR, ''Medicare Provider Analysis and Review (MEDPAR) System No. 09–70–0009.'' We propose to further reduce the scope of activities covered by the NCH with the deletion of two additional sub-files, derived from the Expanded Modified MEDPAR file, known as: ''Quality of Care MEDPAR File (QC/MEDPAR),'' and the ''Medicare Mortality Information File (MMIF).'' The QC/MEDPAR data were initially developed for the purpose of conducting research and effectiveness of care provided in hospitals. The MMIF includes mortality predictors that have been statistically derived by CMS from data provided by the hospital, national data, and the number of previous hospitalizations in all hospitals.

CMS proposes to delete published routine use number 2 authorizing disclosures to the Bureau of the Census; number 5 authorizing disclosures for statistical analysis of inpatient hospital services, number 7 authorizing disclosures to conduct research on QC/MEDPAR data, number 8 authorizing disclosures to an agency of a state government, number 9 authorizing disclosure of data derived from the MMIF, number 10 authorizing disclosures to the Railroad Retirement Board (RRB), number 12 authorizing disclosures to other insurers, number 13 authorizing disclosures to another Federal agency, number 14 authorizing disclosures to states for administration of health care programs, and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA).

Published routine use number 2 is being deleted because it unnecessarily duplicates Exception 4 of the Privacy Act, allowing release of data to the Bureau of the Census. Routine uses number 5, 7, and 9 are no longer needed because they authorize disclosures from the MEDPAR subfiles that are being removed from this system. Disclosures permitted under routine use number 8, 10, 13, 14, and to 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 authorized under published routine use number 12 will be combined with published routine use number 11, which authorizes disclosures to insurance companies. These disclosures to insurance companies will now be covered under proposed routine use number 4.

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

The primary purpose of the SOR is to collect and maintain billing and utilization data on Medicare beneficiaries enrolled in hospital insurance (Part A) or medical insurance (Part B) of the Medicare program for statistical and research purposes related to evaluating and studying the operation and effectiveness of the Medicare program. Information in this system will also be used 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) quality Improvement Organizations (QIO), (4) 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 constituent requests made to a congressional representative, (7) support litigation involving the Agency, and (8) combat fraud and abuse in certain health benefits programs. We have provided background information about the modified system in the ''Supplementary Information'' section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

EFFECTIVE DATES: CMS filed a modified or altered system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on August 2, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered SOR will become effective 30 days from the publication of the notice, or from the date it was submitted to OMB and the congress, whichever is later, unless CMS receives comments that require alterations to this notice.

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

FOR FURTHER INFORMATION CONTACT: Michael Rappaport, Director, Division of Enrollment and Utilization Data Development, Enterprise Databases Group, Office of Information Services, CMS, Room N3–16–28, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–6759.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Background

In 1989, CMS established an SOR titled ''National Claims History, System No. 09–70–0005.'' This system is published at 54 FR 32482 (Aug. 8, 1989). The latest publication of this system was at 59 FR 19181 (April 22, 1994), an unnumbered routine use was added for the Social Security Administration (SSA) at 61 FR 6645 (Feb. 21, 1996), three new fraud and abuse routine uses were added at 63 FR 38414 (July 16, 1998), and at 65 FR 50552 (August 18, 2000), two of the fraud and abuse routine uses were revised and a third deleted.

B. Statutory and Regulatory Basis for System

Authority for maintenance of this SOR is given under the authority of sections 1874(a) and 1875 of the Social Security Act (the Act) and Title 42 United States Code (U.S.C.) 1395(ll).

II. Collection and Maintenance of Data in the System.

A. Scope of the Data Collected

The system contains billing and utilization information on Medicare beneficiaries enrolled in hospital insurance or medical insurance parts of the Medicare program, as well as provider specific information. This system contains name of the beneficiary, residence address, state and county code, mailing zip code, health insurance claim (HIC) number, diagnosis and procedural codes, race, sex, date of birth, as well as the basis for the beneficiary's Medicare entitlement. The system contains provider characteristics and an assigned provider number (facility, referring/servicing physician), admission date, service dates, diagnosis and procedure codes, total charges, Medicare payment amount, and beneficiary's liability.

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 NCH 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 NCH. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. In general, disclosure of information from the SOR will be approved only for the minimum information necessary to accomplish the purpose of the disclosure 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 assist in a variety of health care initiatives with other entities related to the evaluation and study of the operation and effectiveness of the Medicare program.

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. 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 NCH 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 propose 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 pursuant to agreements with CMS to:

a. Contribute to the accuracy of CMS's proper payment of Medicare benefits; and/or

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.

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

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

The Internal Revenue Service may require NCH 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, state agencies in their administration of a Federal health program may require NCH 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 NCH information to enable them to assist in the implementation and maintenance of the Medicare program.

SSA requires NCH data to enable them 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 NCH 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 Quality Improvement Organization (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.

QIOs will work to implement quality improvement programs, provide consultation to CMS, its contractors, and to state agencies. QIOs 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.

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 may require NCH information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided.

5. To an individual or organization for research, evaluation, or epidemiological projects related to the prevention of disease or disability, and the restoration or maintenance of health, or payment related projects.

NCH data will provide for research, evaluations 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.

6. To a Member of Congress or 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 often request the help of a Member of Congress in resolving an issue relating to a matter before CMS. The Member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

7. 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.

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

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.

9. 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 NCH information for the purpose of combating fraud and abuse in such Federally funded programs.

B. Additional Circumstances Affecting Routine Use Disclosures

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 (Dec. 28, 00), as amended by 66 FR 12434 (Feb. 26, 01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.''

In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell

sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

IV. Safeguards

A. Administrative Safeguards

The NCH system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act 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. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems.'' Paragraphs A–C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

Authorized users: Personnel having access to the system have been trained in Privacy Act and systems security requirements. Employees and contractors who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. In addition, CMS is monitoring the authorized users to ensure against excessive or unauthorized use. Records are used in a designated work area or workstation and the system location is attended at all times during working hours.

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

- Database Administrator class owns the database objects; *e.g.*, tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- Quality Indicator 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 individual 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 NCH 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-ons—Authentication is performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.
- Workstation Names—Workstation naming conventions may be defined and implemented at the Agency level.
- Hours of Operation—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the Agency level.
- Inactivity Log-out—Access to the NT workstation is automatically logged out after a specified period of inactivity.
- Warnings—Legal notices and security warnings display on all servers and workstations.
- Remote Access Services (RAS)—Windows NT RAS security handles resource access control. Access to NT resources is controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

C. Procedural Safeguards

All automated systems must comply with Federal laws, guidance, and policies for information systems security as stated previously in this section. Each automated information system should ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

V. Effect of the Modified 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 NCH. Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure. CMS has assigned a higher level of security clearance for the information maintained in this system in an effort to provide added security and protection of data in this system.

CMS will take precautionary measures to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure from the proposed system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act.

CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of the disclosure of information relating to individuals.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0005

SYSTEM NAME:

National Claims History, HHS/CMS/OIS.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive.

SYSTEM LOCATION:

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system contains billing and utilization information on Medicare beneficiaries enrolled in hospital insurance (Part A) or medical insurance (Part B) of the Medicare program.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains Medicare billing and utilization data, name of the beneficiary, health insurance claim (HIC) number, diagnosis and procedural codes, race, sex, date of birth, residence address, state and county code, mailing zip code, as well as the basis for the beneficiary's Medicare entitlement. The system contains provider characteristics, assigned provider number (facility, referring/servicing physician), admission date, service dates, diagnosis and procedure codes, total charges, Medicare payment amount, and beneficiary's liability.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under the authority of sections 1874(a) and 1875 of the Act and Title 42 United States Code (U.S.C.), section 1395 (ll).

PURPOSE(S)

The primary purpose of the SOR is to collect and maintain billing and utilization data on Medicare beneficiaries enrolled in hospital insurance (Part A) or medical insurance (Part B) of the Medicare program for statistical and research purposes related to evaluating and studying the operation and effectiveness of the Medicare program. Information in this system will also be used 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) Quality Improvement Organizations (QIO), (4) 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 constituent requests made to a congressional representative, (7) support litigation involving the Agency, and (8) combat fraud and abuse in certain health benefits programs.

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

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a ''routine use.'' The proposed routine use in this system meets the compatibility requirement of the Privacy Act. In addition, this SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 (Dec. 28, 00), as amended by 66 FR 12434 (Feb. 26, 01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.'' It is also our policy to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary). We are proposing to establish the following routine use disclosures of information that will be maintained in the system:

1. To Agency contractors or consultants who have been 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 pursuant to agreements with CMS to:

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

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.

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 Social Security 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, employers, self-insurers, group health plans, health maintenance organizations, 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 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 third party administrator;

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 research, evaluation, or epidemiological projects related to the prevention of disease or disability, and the restoration or maintenance of health, or payment related projects.

6. To a Member of Congress or 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.

7. 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.

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

9. 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:

Records are stored on both tape cartridges (magnetic storage media) and in a DB2 relational database management environment (DASD data storage media).

RETRIEVABILITY:

Information is most frequently retrieved by HIC, provider number (facility, physician, supplier IDs), service dates, type of bill, Medicare status code, diagnoses, procedure codes, and beneficiary state code.

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

RETENTION AND DISPOSAL:

Records are maintained with identifiers for all transactions after they are entered into the system for a period of 20 years. Records are housed in both active and archival files.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Enrollment and Utilization Data Development, Enterprise Databases Group, Office of Information Services, CMS, Room N3–16–28, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of notification, the subject individual should write to the system manager who will require the system name, and the retrieval selection criteria (e.g., HIC, facility ID, physician/supplier number, service dates, type of bill, etc.).

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7).

RECORD SOURCE CATEGORIES:

Fee-for-Service (FFS) billing and utilization information contained in this records system is obtained from the Common Working File, System No. 09–70–0526. Medicare+Choice (M+C) organization utilization information to be contained in this records system will be obtained from a single front-end processor that will function as both a Fiscal Intermediary (System No. 09–70–0503) and Carrier (System No. 09–70–0501).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–22741 Filed 9–5–02; 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 New System

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

ACTION: Notice of new system of records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system of records, called the ''Correspondence Tracking Management System (CTMS),'' HHS/CMS/OSORA No. 09–70–3005. The CMTS replaces the Correspondence and Assignment Tracking and Control System (CATCS), System No. 09–70–9001 that was deleted from CMS' database inventory through a published notice in the **Federal Register**. The primary purpose of the system of records is to aid CMS in tracking incoming correspondence about CMS programs from the Office of the Secretary, Medicare beneficiaries and Medicaid recipients. In addition, it will track all correspondence from the public, other government agencies, contractors, and members of the Congress. Information retrieved from this system of records will be used to support regulatory, reimbursement, and policy functions performed within the agency or by a contractor or consultant; support constituent requests made to a Congressional representative; and support litigation involving the agency.

We have provided background information about the proposed system in the ''Supplementary Information'' section, below. Although the Privacy Act requires only that the ''routine use'' portion of the system be published for comment, CMS invites comments on all portions of this notice. See ''Effective Dates'' section for comment period.

EFFECTIVE DATES: CMS filed a new system report with the Chair of the House Committee on Government