

Health Policy, Rutgers University; Dr. Everard Rutledge, Vice President of Community Health, Bon Secours Health Systems, Inc.; Jay Sackman, Executive Vice President, 1199 Service Employees International Union; Dallas Salisbury, President and Chief Executive Officer, Employee Benefit Research Institute; Rosemarie Sweeney, Vice President, Socioeconomic Affairs and Policy Analysis, American Academy of Family Physicians; and Bruce Taylor, Director, Employee Benefit Policy and Plans, Verizon Communications.

The agenda for the September 26, 2002 meeting will include the following:

- Recap of the previous (May 23, 2002) meeting.
- *Medicare & You* Campaign update.
- Update on 2002 Medicare National Multi-Media and Education Campaign.
- CMS quality initiative.
- Briefing on *www.medicare.gov*.
- Listening session with the Administrator.
- Public comment.

Individuals or organizations that wish to make a 5-minute oral presentation on an agenda topic should contact Ms. Caliman by 12 noon, September 19, 2002. A written copy of the oral presentation should also be submitted to Ms. Caliman by 12 noon, September 19, 2002. The number of oral presentations may be limited by the time available. Individuals not wishing to make a presentation may submit written comments to Ms. Caliman by 12 noon, September 19, 2002. The meeting is open to the public, but attendance is limited to the space available. Individuals requiring sign language interpretation for the hearing impaired or other special accommodations should contact Ms. Caliman at least 15 days before the meeting.

Authority: Sec. 222 of the Public Health Service Act (42 U.S.C. 217(a) and sec. 10(a) of Pub. L. 92-463 (5 U.S.C. App. 2, sec. 10(a) and 41 CFR 102-3). (Catalog of Federal Domestic Assistance Program No. 93.733, Medicare—Hospital Insurance Program; and Program No. 93.774, Medicare—Supplementary Medical Insurance Program)

Dated: July 15, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

[FR Doc. 02-18613 Filed 7-25-02; 8:45 am]

BILLING CODE 4120-01-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.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter a system of records, "Medicaid Statistical Information System (MSIS), System No. 09-70-6001." We propose to delete published routine use number 1 pertaining to a contractor, number 5 pertaining to employees of a state government, number 6 pertaining to another Federal agency, and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA). Disclosures previously covered by routine uses number 5, 6, and to the SSA will be accomplished by adding a new routine use number 2 which authorizes release of information in this system to "another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent." We propose to modify the language of routine use number 1 to clarify the circumstances for disclosure under this routine use and retain the proposed placement of this routine use as number 1.

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

The primary purpose of the system of records is to establish an accurate, current, and comprehensive database containing standardized enrollment, eligibility, and paid claims of Medicaid beneficiaries to be used for the

administration of Medicaid at the Federal level, produce statistical reports, support Medicaid related research, and assist in the detection of fraud and abuse in the Medicare and Medicaid programs. Information in this system will also be used to: Support regulatory and policy functions performed within the Agency or by a contractor or consultant, another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent, support research of policy issues, quality and effectiveness of care, and of epidemiological projects, support constituent requests made to a congressional representative, support litigation involving the Agency related to this system of records, and combat fraud and abuse in certain Federally funded health benefits programs. We have provided background information about the modified system in the **SUPPLEMENTARY INFORMATION** section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the 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 July 5, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered system of records, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution, 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: Ron North, Technical Advisor, Division of Informational Analysis and Technical Assistance, Center for Medicaid and State Operations, CMS, Room S3-17-26, 7500 Security Boulevard, Baltimore, Maryland 21244-1850. The telephone number is 410-786-5651.

SUPPLEMENTARY INFORMATION:**I. Description of the Modified System of Records***Statutory and Regulatory Basis For System of Records*

In 1994, CMS established a system of records under the authority of § 1902 (a)(6) of the Social Security Act (the Act)(42 Code of Federal Regulations (CFR) 1396a(a)(6)), and the Balanced Budget Act (Public Law 105-33). Notice of this system, MSIS, System No. 09-70-6001," was published in the **Federal Register** at 59 FR 41327 (Aug. 11, 1994), an unnumbered routine use was added for SSA at 61 FR 6645 (Feb. 21, 1996), three new fraud and abuse routine uses were added at 63 FR 38414 (July 16, 1998), and then at 65 FR 50552 (Aug. 18, 2000), two of the fraud and abuse routine uses were revised and a third deleted.

II. Collection and Maintenance of Data in the System*A. Scope of the Data Collected*

The system contains information concerning Medicaid beneficiaries, physicians, and other providers of services to Medicaid beneficiaries. Information on beneficiaries consist of an assigned Medicaid identification number, social security number (SSN), health insurance claims number (HICN), date of birth, sex, ethnicity and race, medical services, equipment, and supplies for which Medicaid reimbursement is requested, and materials used to determine amount of benefits allowable under Medicaid. Information on physicians and other providers of services to the beneficiary consist of an assigned provider identification number, and information used to determine whether a sanction or suspension is warranted.

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 MSIS 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 MSIS. CMS has the following policies and procedures concerning

disclosures of information that will be maintained in the system. Disclosure of information from the system of records will be approved only for the minimum information necessary to accomplish the purpose of the disclosure only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, *e.g.*, establish an accurate, current, and comprehensive database for administration of the Medicaid program at the Federal level, produce statistical reports, support Medicaid related research, and assist in the detection of fraud and abuse in the Medicaid 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.

5. 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.

6. 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.

7. 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.

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 MSIS 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 engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system of records 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 system of records.

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 management of Medicare/Medicaid 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; and/or
 - c. To assist Federal/state Medicaid programs within the state.

Other Federal or state agencies in their administration of a Federal health program may require MSIS information for the purposes of determining, evaluating and/or assessing cost, effectiveness, and /or the quality of health care services provided in the state.

SSA may require MSIS data to enable them to assist in the implementation and maintenance of the Medicare/Medicaid program.

Disclosure under this routine use shall be used by state Medicaid agencies pursuant to agreements with HHS for determining Medicaid and Medicare eligibility, for quality control studies, for determining eligibility of recipients of assistance under Titles IV, XVIII, XIX and XXI of the Act, and for the administration of the Medicaid program.

Data will be released to the state only on those individuals who are eligibly enrollees, and beneficiaries 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 MSIS 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 system of records.

3. 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.

MSIS data will provide for the research, evaluations, and epidemiological projects, a broader, longitudinal, national perspective of the status of Medicaid 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/Medicaid beneficiaries and the policy that governs the care.

4. 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.

Individuals 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.

5. 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.

6. 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.

7. 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 MSIS 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 MSIS system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, the Clinger-Cohen Act of 1996, and OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." CMS has prepared a comprehensive system security plan as required by the Office and Management and Budget (OMB) Circular A-130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," Paragraphs A-C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

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

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

database configuration includes five classes of database users:

- Database Administrator class owns the database objects; *e.g.*, tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- Quality Indicator (QI) Report Generator class has read-only access to all fields and tables;
- Policy Research class has query access to tables, but are not allowed to access confidential 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 MSIS 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 (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-ons—Authentication is performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.
- Workstation Names—Workstation naming conventions may be defined and implemented at the Agency level.
- Hours of Operation—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the Agency level.

- Inactivity Log-out—Access to the NT workstation is automatically logged out after a specified period of inactivity.

- Warnings—Legal notices and security warnings display on all servers and workstations.

- Remote Access Services (RAS)—Windows NT RAS security handles resource access control. Access to NT resources is controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

C. Procedural Safeguards:

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

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

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CMS will monitor the collection and reporting of MSIS data. MSIS information on individuals is completed by contractor personnel and submitted to CMS through standard systems located at different locations. CMS will utilize a variety of onsite and offsite edits and audits to increase the accuracy of MSIS data.

CMS will take precautionary measures (*see* item IV. above) 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 of identifiable data from the modified 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: July 5, 2002.

Thomas A. Scully,
Administrator, Centers for Medicare & Medicaid Services.

System No. 09-70-6001

SYSTEM NAME:

Medicaid Statistical Information System (MSIS), HHS/CMS/CMSO.

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 information on Medicaid beneficiaries, and physicians and other providers involved in furnishing services to Medicaid beneficiaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information contained in this system include an assigned Medicaid identification number, social security number (SSN), health insurance claims number (HIC), date of birth, sex, ethnicity and race, medical services, equipment, and supplies for which Medicaid reimbursement is requested, and materials used to determine amount of benefits allowable under Medicaid. Information on physicians and other providers of services to the beneficiary consist of an assigned provider identification number, and information used to determine whether a sanction or suspension is warranted.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for the maintenance of this system of records is given under § 1902 (a)(6) of the Social Security Act (42 United States Code (U.S.C.) § 1396a (a)(6), and the Balanced Budget Act (Public Law 105-33).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the system of records is to establish an accurate, current, and comprehensive database containing standardized enrollment, eligibility, and paid claims of Medicaid beneficiaries to be used for the administration of Medicaid at the Federal level, produce statistical reports, support Medicaid related research, and assist in the detection of fraud and abuse in the Medicaid program. Information in this system will also be used to: support regulatory and policy functions performed within the

Agency or by a contractor or consultant, another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent, support research of policy issues, quality and effectiveness of care, and of epidemiological projects, support constituent requests made to a congressional representative, support litigation involving the Agency related to this system of records, and combat fraud and abuse in certain Federally funded health benefits programs.

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

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a "routine use." The proposed routine use in this system meets the compatibility requirement of the Privacy Act.

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

In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary). We are proposing to establish the following routine use disclosures of information that will be maintained in the system:

1. To Agency contractors, or consultants who have been engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system of records 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 management of Medicare/Medicaid 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; and/or

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

3. 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.

4. 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.

5. 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.

6. To 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.

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

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

STORAGE:

Computer diskette and on magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by the assigned beneficiary identification number, SSN, HICN, and the assigned physician or other providers of services identification number.

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

RETENTION AND DISPOSAL:

Records are maintained in a secure storage area with identifiers. Disposal occurs ten years after the final determination of the case is completed.

SYSTEM MANAGER AND ADDRESS:

Director, Division of Informational Analysis and Technical Assistance, Center for Medicaid and State Operations, CMS, Room S3-18-17, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system

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

RECORD ACCESS PROCEDURE:

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

CONTESTING RECORD PROCEDURES:

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

RECORD SOURCE CATEGORIES:

CMS obtains the identifying information contained in this system from state Medicaid agencies, or Medicaid Management Information Systems maintained by the individual states, and information contained on CMS Form 2082.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02-18170 Filed 7-25-02; 8:45 am]

BILLING CODE 4120-03-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of Modified or Altered System

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

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

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter an SOR, "Individuals Authorized Access to the CMS Data Center, System No. 09-70-0064." We propose to amend the name of this system to more accurately

reflect the purpose of this system to read "Individuals Authorized Access to the CMS Computer Services (IACS)." We propose to delete an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA). Disclosure of data from this system to the SSA is no longer necessary since SSA has been established as a separate agency outside of the HHS and a routine use for the purpose stated is no longer necessary.

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 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 for assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. Information in this system will be used will be used to support regulatory and policy functions performed within the Agency or by a contractor or consultant; support constituent requests made to a Congressional representative; and to support litigation involving the Agency related to this SOR. 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 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 July 19, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless

CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution (DDL), 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: Kenneth Olga, Technology Services Group, Office of Information Services, CMS, Room N1-19-18, 7500 Security Boulevard, Baltimore, Maryland 21244-1850. The telephone number is 410-786-4067.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Statutory and Regulatory Basis For SOR

In 1994, CMS established an SOR under the authority of 5 U.S.C. 5552(e)(10). Notice of this system, "Individuals Authorized Access to the CMS Data Center, System No. 09-70-0064," was published at 59 **Federal Register** (FR) 41330 (Aug. 11, 1994).

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system contains the name, work address, work phone number, an assigned user identification (UserID) number, an associated password, and the software system(s) that the individual is authorized to use.

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 IACS information that can be associated with an individual as provided for under "Section III.A. Entities Who May Receive Disclosures Under Routine Use." Both identifiable and non-identifiable data may be disclosed under a routine use. Identifiable data includes individual records with IACS information and identifiers. Non-identifiable data includes individual records with IACS information and masked identifiers or IACS information with identifiers stripped out of the file.

We will only disclose the minimum personal data necessary to achieve the