EFFECTIVE DATE: July 15, 2002.

FOR FURTHER INFORMATION CONTACT: Rich Robuck, Readiness, Response and Recovery and Directorate, Federal Emergency Management Agency, Washington, DC 20472, (202) 646–2705 or *Rich.Robuck@fema.gov.*

SUPPLEMENTARY INFORMATION: The notice of a major disaster declaration for the State of Minnesota is hereby amended to include the following areas among those areas determined to have been adversely affected by the catastrophe declared a major disaster by the President in his declaration of June 14, 2002:

Goodhue and Hubbard Counties for Public Assistance.

Itasca, McLeod, and Wright Counties for Public Assistance (already designated for Individual Assistance).

(The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 83.537, Community Disaster Loans; 83.538, Cora Brown Fund Program; 83.539, Crisis Counseling; 83.540, Disaster Legal Services Program; 83.541, Disaster Unemployment Assistance (DUA); 83.542, Fire Suppression Assistance; 83.543, Individual and Family Grant (IFG) Program; 83.544, Public Assistance Grants; 83.545, Disaster Housing Program; 83.548, Hazard Mitigation Grant Program)

Joe M. Allbaugh,

Director.

[FR Doc. 02–18526 Filed 7–22–02; 8:45 am]

BILLING CODE 6718–02–P

FEDERAL EMERGENCY MANAGEMENT AGENCY

[FEMA–1425–DR]

Texas; Amendment No. 4 to Notice of a Major Disaster Declaration

AGENCY: Federal Emergency Management Agency (FEMA).

ACTION: Notice.

SUMMARY: This notice amends the notice of a major disaster for the State of Texas, (FEMA–1425-DR), dated July 4, 2002, and related determinations.

EFFECTIVE DATE: July 15, 2002.

FOR FURTHER INFORMATION CONTACT: Rich Robuck, Readiness, Response and Recovery Directorate, Federal Emergency Management Agency, Washington, DC 20472, (202) 646–2705 or *Rich.Robuck@fema.gov.*

SUPPLEMENTARY INFORMATION: Notice is hereby given that, effective this date and pursuant to the authority vested in the Director of the Federal Emergency Management Agency under Executive Order 12148, I hereby appoint Scott Wells of the Federal Emergency Management Agency to act as the Federal Coordinating Officer for this declared disaster.

This action terminates my appointment of Sandra L. Coachman as Federal Coordinating Officer for this disaster.

(The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 83.537, Community Disaster Loans; 83.538, Cora Brown Fund Program; 83.539, Crisis Counseling; 83.540, Disaster Legal Services Program; 83.541, Disaster Unemployment Assistance (DUA); 83.542, Fire Suppression Assistance; 83.543, Individual and Family Grant (IFG) Program; 83.544, Public Assistance Grants; 83.545, Disaster Housing Program; 83.548, Hazard Mitigation Grant Program)

Joe M. Allbaugh,

Director.

[FR Doc. 02–18525 Filed 7–22–02; 8:45 am]

BILLING CODE 6718–02–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, ''Medicare Health Maintenance Organizations/Competitive Medical Plans Beneficiary Reconsideration System (MBRS),'' System No. 09–70–4003. We propose to change the name of the system to read ''Medicare Managed Care Beneficiary Reconsideration (RECON) System,'' to reflect the change in the programs related to this activity. The language in published routine use number 3 will be modified to more accurately reflect activities currently performed by contractors and consultants. We propose to delete published routine use number 5, pertaining to '' a state insurance commissioner * * *'' and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA). Access to the data for these activities will be accomplished by adding a new routine use 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.'' Disclosure of information to Quality Improvement Organizations (QIO) (formerly Peer Review Organizations) as stated in published routine use number 5 will be treated as a new routine use and prioritized as routine use number 4. We propose to modify the language of published routine use number 4 pertaining to ''a third party'' to limit disclosures authorized under this routine use and to provide clarity to the circumstances for disclosures. Third parties will be treated as a new routine use and prioritized as routine use number 3.

The security classification previously reported as ''None'' will be modified to reflect that the 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'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 recent reorganizations and to update language in the administrative sections to correspond with language used in other CMS SORs.

The primary purpose of the system is to collect and maintain information necessary to process requests for reconsideration of service requests or claims by or on behalf of Medicare managed care enrollees, promote the effectiveness and integrity of the Medicare managed care program, and reply to future correspondence related to the case. Information in this system will also be disclosed to: (1) Support regulatory and policy functions performed within the Agency or by a contractor or consultant, (2) another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, (3) third party contacts, (4) QIOs, (5) support constituent requests made to a congressional representative, (6) support litigation involving the Agency related to this SOR, and (7) combat fraud and abuse in certain health care 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 June 17, 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 standard time.

FOR FURTHER INFORMATION CONTACT: Beverly Sgroi, Health Insurance Specialist, Division of Hearings, Appeals & Dispute Resolution, Center for Beneficiary Choices, CMS, Mail-stop S1–05–06, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–7638. The e-mail address is *bsgroi@hhs.cms.gov*.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System of Records.

A. Statutory and Regulatory Basis for SOR

In 1988, CMS established an SOR under the authority of § 1872 of the Social Security Act (the Act) (Title 42 United States Code (U.C.S. section 1395mm). Notice of this system, MBRS, was published in the **Federal Register** (FR) 53 FR 35914 (Sept. 15, 1988), a 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 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 Medicare beneficiaries who have been enrolled in a managed care program and who have requested an appeal by CMS, or any person who acts on behalf of these beneficiaries. The system contains the name and address of beneficiaries and the individual representing the beneficiary in this appeal process. It will also contain the beneficiary's social security number (SSN), health insurance claims number (HIC), health insurance plan name and address, health insurance plan number, medical records and statement of fact, service requests/claims data, date of service request/claim received by the health plan, dates of service, beneficiary enrollment form and disenrollment form, verification of enrollment status, date reconsideration request submitted to CMS, and dates of determination by plan and CMS.

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

We will only collect the minimum personal data necessary to achieve the purpose of RECON. 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 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., collecting and maintaining information used in processing the claimant's appeal and information necessary to reply to future correspondence.

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

In addition, other state agencies in their administration of a Federal health program may require RECON 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 requires RECON data to enable them to assist in the implementation and maintenance of the Medicare program.

State Insurance Commissioners or other state regulators with similar authority acting in a manner consistent with maintaining the integrity of the Medicare program may require RECON data to assist in accomplishing their activities.

3. 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 exists, 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, or any case 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 party contacts require RECON 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.

4. To Quality Improvement Organizations (QIO) 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.

5. 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.

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

a. The Agency or any component thereof, or

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

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

d. The United States Government,

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

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.

7. 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.

8. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to investigate potential fraud 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 RECON 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 (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 RECON 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 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 RECON 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 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 RECON data. RECON 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 RECON 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: June 17, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

System No. 09–70–4003

SYSTEM NAME:

Medicare Managed Care Beneficiary Reconsideration (RECON) System No. 09–70–4003.

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 concerning Medicare beneficiaries who have been enrolled in a managed care program and who have requested an appeal by CMS, or any person who acts on behalf of these beneficiaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains the name and address of beneficiaries and the individual representing the beneficiary in this appeal process. It will also contain the beneficiary's social security number (SSN), health insurance claims number (HIC), health insurance plan name and address, health insurance plan number, medical records and statement of fact, service requests/claims data, date of service request/claim received by the health plan, dates of service, beneficiary enrollment form and disenrollment form, verification of enrollment status, date reconsideration request submitted to CMS, and dates of determination by plan and CMS.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for the maintenance of this system of records is given under §§ 1852, and 1876 of the Social Security Act (the Act) United States Code (U.S.C.) §§ 1395w–22, and 1395mm).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the SOR is to collect and maintain information necessary to process requests for reconsideration of service requests or claims by or on behalf of Medicare managed care enrollees, promote the effectiveness and integrity of the Medicare managed care program, and reply to future correspondence related to the case. Information in this system will also be disclosed to: (1) Support regulatory and policy functions performed within the Agency or by a contractor or consultant, (2) another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, (3) third party contacts, (4) Quality Improvement Organizations (QIO) (formerly Peer Review Organizations), (5) support constituent requests made to a congressional representative, (6) support litigation involving the Agency related to this SOR, and (7) combat fraud and abuse in certain health care 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 RECON 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.

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). We are proposing to establish or modify the following routine uses for disclosures of information maintained in the system:

1. 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 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 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 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 exists, 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, or any case 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.

4. To Quality Improvement Organizations 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.

5. 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.

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

a. The Agency or any component thereof, or

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

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

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

7. 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.

8. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to investigate potential fraud 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 name, SSN, and/or HICN of claimant.

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 RECON 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 Information Systems Security Policy, Standards, and Guidelines Handbook, and OMB Circular No. A–130, Appendix III.

RETENTION AND DISPOSAL:

Records are maintained in a secure storage area with identifiers. Case records are transferred to and maintained in an archival file for a period of 15 years.

SYSTEM MANAGER AND ADDRESS:

Director, Division of hearings, Appeals & Dispute Resolution, Center for Beneficiary Choices, CMS, 7500 Security Boulevard, Mailstop 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, HIC, address, 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:

Sources of information contained in this records system is obtained from the reconsideration requests made by or on behalf of Medicare beneficiaries and from inquiries from congressional offices, health plans, providers, state insurance commissioners, state regulators, disenrollment surveys, Medicare carriers or intermediaries, and QIO records.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–18167 Filed 7–22–02; 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: 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, ''Medicare Supplier Identification File (MSIF), System No. 09–70–0530.'' We are deleting routine uses number 2 pertaining to a Medicaid state agency or its fiscal agent to assist in enforcing Medicare and Medicaid sanctions, and number 4 pertaining to contractors. Disclosures previously allowed by routine use number 2 pertaining to a Medicaid state agency will now be covered by proposed routine use number 5. Disclosures previously allowed by routine use number 4 pertaining to contractors will now be covered by proposed routine use