facilities, workers at DOE facilities, and other persons potentially exposed to radiation or to potential hazards from non-nuclear energy production use. HHS delegated program responsibility to CDC.

In addition, a memo was signed in October 1990 and renewed in November 1992, 1996, and in 2000, between ATSDR and DOE. The MOU delineates the responsibilities and procedures for ATSDR's public health activities at DOE sites required under sections 104, 105, 107, and 120 of the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA or ''Superfund''). These activities include health consultations and public health assessments at DOE sites listed on, or proposed for, the Superfund National Priorities List and at sites that are the subject of petitions from the public; and other health-related activities such as epidemiologic studies, health surveillance, exposure and disease registries, health education, substance-specific applied research, emergency response, and preparation of toxicological profiles.

Purpose: This subcommittee is charged with providing advice and recommendations to the Director, CDC, and the Administrator ATSDR, regarding community concerns pertaining to CDC's and ATSDR's public health activities and research at this DOE site. The purpose of this meeting is to provide a forum for community interaction and serve as a vehicle for community concerns to be expressed as advice and recommendations to CDC and ATSDR.

Matters to be Discussed: Agenda items include an update from the National Institute for Occupational Safety and Health (NIOSH); a presentation on toxicity of heavy metals and radionuclides; an update on screening methods for Savannah River Site production workers; and status reports from the SRSHES working groups on Epidemiologic Data, Scenario Screening, and Phase II—Community Summary.

Agenda items are subject to change as priorities dictate.

An administrative delay prevented meeting the 15-day publication requirement.

Contact Person for More Information: Phillip Green, Executive Secretary, SRSHES, Radiation Studies Branch, Division of Environmental Hazards and Health Effects, NCEH, CDC, 1600 Clifton Road, N.E. (E–39), Atlanta, GA 30333, telephone 404/498–1800, fax 404/498–1811.

The Director, Management Analysis and Services Office, has been delegated the authority to sign Federal Register notices pertaining to announcements of meetings and other committee management activities for both CDC and ATSDR.

Dated: December 19, 2001.

John Burckhardt,

Acting Director, Management Analysis and Services Office, Centers for Disease Control and Prevention.

[FR Doc. 01–31733 Filed 12–26–01; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of a 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 titled ''Home Health Agency Outcome and Assessment Information Set (HHA OASIS),'' System No. 09–70–9002. CMS proposes to add a new routine use authorizing disclosure to national accrediting organizations that have been approved by CMS for deeming authority for Medicare requirements for home health services. Information will be released to these organizations upon specific request, and only for those facilities that they accredit and that participate in the Medicare program by virtue of their accreditation status, *i.e.,* facilities with deemed status. Additionally, disclosures authorized by published routine uses numbers 3 and 4 are similar in scope and as such will be combined into one routine use to allow 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, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations.'' CMS will also add 2 new routine uses that will permit disclosure of information in this system to combat fraud and abuse in certain Federally funded health care programs.

In addition, 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 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 purposes of the SOR are to: (1) Study and help ensure the quality of care provided by home health agencies (HHA); (2) aid in administration of the survey and certification of Medicare/Medicaid HHAs; (3) enable regulators to provide HHAs with data for their internal quality improvement activities; (4) support agencies of the state government to determine, evaluate and assess overall effectiveness and quality of HHA services provided in the state; (5) provide for the validation, and refinements of the Medicare Prospective Payment System; (6) aid in the administration of Federal and state HHA programs within the state; and (7) monitor the continuity of care for patients who reside temporarily outside of the state. Information maintained in this system will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) assist another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations; (3) support research, evaluation, or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects; (4) support the functions of Peer Review Organizations (PRO); (5) support the functions of national accrediting organizations; (6) support litigation involving the Agency; (7) support constituent requests made to a Congressional representative; and (8) combat fraud and abuse in certain health care programs. 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 SOR report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on December 18, 2001. The modified SOR, including routine uses, will become effective 40 days from the publication of this notice, or from the date it was submitted to OMB and the Congress, whichever is later. We may defer implementation of this SOR or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution (DDLD), 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: Helene Fredeking, Technical Director, Division of Nursing Homes and Continuing Care Services, Center for Medicaid and State Operations, CMS, 7500 Security Boulevard, S2–12–25, Baltimore, Maryland 21244–1850. The telephone number is (410) 786–7304.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Background

CMS established a new SOR in 1999 containing data on the physical, mental, functional, and psychosocial status of all patients receiving the services of HHAs that are approved to participate in the Medicare and/or Medicaid programs. Information retained in this system for those individuals who have only non-Medicare and non-Medicaid payment sources will be in a non-patient identifiable format. Notice of this system was published in the **Federal Register** at 64 **Federal Register** (FR) 32992 (June 18, 1999). We published in the **Federal Register**, at 62 FR 11035 (March 10, 1997), a proposed rule with an opportunity for public comment, titled ''Medicare and Medicaid Programs: Use of the OASIS as Part of the Conditions of Participation for Home Health Agencies.'' Some provisions of this rule were published as a Final Rule in the **Federal Register** at 64 FR 3764 (January 25, 1999) titled ''Medicare and Medicaid Program: Comprehensive Assessment and Use of the OASIS as Part of the Conditions of Participation for Home Health Agencies.''

The rule required that all HHAs participating in the Medicare and Medicaid programs be required to complete a standard, valid, patient assessment data set; i.e., the OASIS, as part of their comprehensive assessments and updates when evaluating adult, non-maternity patients as required by section 484.55 of the Conditions of Participation. Also published in the **Federal Register** at 64 FR 3748 (January 25, 1999) was an interim final rule with comment titled ''Medicare and Medicaid: Reporting Outcome and Assessment Information Set (OASIS) Data as Part of the Conditions of Participation for Home Health Agencies.'' This interim rule established an additional requirement of the Conditions of Participation for HHAs approved to participate in Medicare and/or Medicaid, to encode and report OASIS electronically into a national database. Information retained in this system for those individuals who have only non-Medicare and non-Medicaid payment sources will be in a non-patient identifiable format and will be used only for statistical purposes and to ensure quality of care for all patients. Information on Medicare and Medicaid patients will be identified for quality of care and reimbursement purposes.

B.Statutory and Regulatory Basis for SOR

Sections 1102(a), 1154, 1861(m), 1861(o), 1861(z), 1863, 1864, 1865, 1866, 1871, 1891, and 1902 of the Social Security Act (the Act) authorize the Administrator of CMS to require HHAs participating in the Medicare and Medicaid programs to complete a standard, valid, patient assessment data set; i.e., the OASIS, as part of their comprehensive assessments and updates when evaluating adult, non-maternity patients as required by section 484.55 of the Conditions of Participation.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The OASIS will be completed on all patients, except those in a category exempted by administrative policies and procedures, who receive services from an HHA certified for Medicare and Medicaid payments. The OASIS data set includes identifiers. It also includes information on: (1) Patient History, (2) Living Arrangements, (3) Supportive Assistance, (4) Sensory Status, (5) Integumentary Status, (6) Respiratory Status, (7) Elimination Status, (8) Neuro/Emotional/Behavioral Status, (9) Activities of Daily Living/Instrumental Activities of Daily Living (ADL/IADL), (10) Medications, (11) Equipment Management, (12) Emergent Care, and (13) Discharge. Identifiers are patient name, social security number, Medicare number and Medicaid number. A masked identifier is one in which an encrypted value is permanently substituted for an identifier to prevent recipients of the information from identifying the individual.

The OASIS information will be submitted by the HHA to the government for all patients, except pre-partum and postpartum patients, patients under 18 years of age, and patients receiving other than personal care or health care services; i.e., housekeeping services and chore services. Identifiers will be included for all patients receiving services paid for by Medicare traditional fee-for-service, Medicaid traditional fee-for-service, Medicare HMO/managed care or Medicaid HMO/managed care. For patients with only a non-Medicare or non-Medicaid payment source, the HHA will submit OASIS information with masked identifiers and will retain the identifier and masked identifier at the HHA. In other words, the patient identifier for non-Medicare and non-Medicaid patients will only be known and retained by the HHA and not by the government.

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 OASIS information that can be associated with an individual HHA patient as provided for under ''Section III. 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 OASIS information and identifiers. Non-identifiable data includes individual records with OASIS information and masked identifiers or OASIS information with identifiers stripped out of the file.

We will only disclose the minimum personal data necessary to achieve the purpose of OASIS. 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 after CMS:

Determines that the use or disclosure is consistent with the reason that the data is being collected; e.g., study and help ensure the quality of care provided by HHAs, developing and refining payment systems, and monitoring the quality of care provided to patients.

1. 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).

2. Requires the information recipient to:

a. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

b. remove or destroy at the earliest time all patient-identifiable information; and

c. agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

3. 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 OASIS without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, or consultants who have been contracted by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system 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, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations 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 (e.g., state survey agencies and state Medicaid agencies) may require OASIS data to contribute to the accuracy of CMS's health insurance operations (payment, treatment and coverage) and/or to support state agencies in the evaluations and monitoring of care provided by HHAs;

Other Federal or state agencies may require OASIS data for purposes of determining, evaluating and/or assessing overall or aggregate cost, effectiveness, and/or the quality of HHA services provided in the state;

Other Federal or state agencies may require OASIS data for developing and operating Medicaid reimbursement systems or for the purpose of administration of Federal/state HHA programs within the state. Data will be released to the state only on those individuals who are either patients under the services of an HHA within the state, or are legal residents of the state, regardless of the location of the HHA in which the patient is receiving services.

State government components in partnership with CMS will use OASIS information to enhance the monitoring of HHAs' performance in providing patient care. States will also use this information to study the cost effectiveness and quality of Medicaid programs. In addition some states will use OASIS information for case mix Medicaid reimbursement systems. States will use OASIS data to monitor the continuity of care delivered to patients who, for whatever reason, temporarily reside in another state and receive HHA services during that stay.

Other state agencies in their administration of a Federal health program may require OASIS information in order to support evaluations and monitoring of quality of care for special populations or special care area, including proper reimbursement for services provided. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purpose for which CMS collects the information.

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.

The OASIS data will provide the research, evaluations and epidemiological projects a broader, longitudinal, national perspective of the status of HHA patients. CMS anticipates that many researchers will have legitimate requests to use these data in projects that could ultimately improve the care provided to HHA patients and the policy that governs the care.

4. To PROs in order to assist the PRO to perform Title XI and Title XVIII functions relating to assessing and improving HHA quality of care.

PROs will work with HHAs to implement quality improvement programs, provide consultation to CMS, its contractors, and to state agencies. The PROs will provide a supportive role to HHAs in their endeavors to comply with Medicare Conditions of Participation; will assist the state agencies in related monitoring and enforcement efforts; assist CMS and help regional home health intermediaries in home health program integrity assessment; and prepare summary information about the nation's home health care for release to beneficiaries.

5. To national accrediting organizations with approval for deeming authority for Medicare requirements for

home health services (i.e., the Joint Commission on Accreditation of Healthcare Organizations, or the Community Health Accreditation Program). Information will be released to these organizations upon specific request, and only for those facilities that they accredit, and that participate in the Medicare program by virtue of their accreditation (deemed) status.

CMS anticipates providing these national accrediting organizations with OASIS information to enable them to target potential or identified problems during the organization's accreditation review process of that facility.

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 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 some 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.

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 programs.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contract or grant with a third party to assist in accomplishing CMS functions relating to the purpose of combating fraud and abuse;

CMS occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or grantee whatever information is necessary for the contractor or grantee to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or grantee from using or disclosing the information for any purpose other than that described in the contract and requiring the contractor or grantee to return or destroy all information.

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

B. Additional Circumstances Affecting Routine Use Disclosure

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 **Federal Register** 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 this HHS regulation ''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

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

A. Authorized Users

Personnel having access to the system have been trained in 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 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 state 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 Index Report Generator* class has read-only access to all fields and tables;
- *Policy Research* class has query access to tables, but are not allowed to access confidential patient identification information; and

• *Submitter* class has read and write access to database objects, but no database administration privileges. This class is used by the OASIS data submission applications to receive and validate HHA file uploads.

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 HHA OASIS 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 state 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 state agency level.

• Inactivity Lockout—Access to the NT workstation is automatically locked after a specified period of inactivity.

• Warnings—Legal notices and security warnings display on all servers and when servers are accessed by workstations.

• Remote Access Security—Windows NT Remote Access Service (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.

There are several levels of security found in the HHA OASIS system. Windows NT provides much of the overall system security. The Windows NT security model is designed to meet the C2-level criteria as defined by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria document (DoD 5200.28–STD, December 1985). Netscape Enterprise Server is the security mechanism for all HHA transmission connections to the system. As a result, Netscape controls all HHA information access requests. Anti-virus software is applied at both the workstation and NT server levels. Access to different areas on the Windows NT server are maintained through the use of file, directory and share level permissions. These different levels of access control provide security that is managed at the user and group level within the NT domain. The file and directory level access controls rely on the presence of an NT File System hard drive partition. This provides the most robust security and is tied directly to the file system. Windows NT security is applied at both the workstation and NT server levels.

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 established 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. CMS has assigned a higher level of security clearance for the information in this system to provide added security and protection of data in this system.

CMS will monitor the collection and reporting of OASIS data. OASIS information on patients is completed by the HHA and submitted to CMS through standard systems located at the state agencies. Accuracy of the data is important since incorrect information could result in the wrong reimbursement for services and a less effective process for assuring quality of services. CMS will utilize a variety of onsite and offsite edits and audits to increase the accuracy of OASIS 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 including not collecting patient identifiable data for non-Medicare and non-Medicaid patients. Therefore, CMS anticipates no adverse effect on any of these 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 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.

To secure data that resides in a CMS Privacy Act SOR; to ensure the integrity, security, and confidentiality of information maintained by CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and the non-CMS recipient of the data (hereafter termed User), enter into an agreement to comply with the following specific requirements. The agreement addresses the conditions under which CMS will disclose and the User will obtain and use the information contained in the system. The parties mutually agree that CMS retains ownership rights to the data and that the User does not obtain any right, title, or interest in any of the data furnished by CMS. The User represents and warrants further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. The User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data disclosed from the SOR to any person. The User agrees that access to the data shall be limited to the minimum number of individuals necessary to achieve the purpose stated in the protocol and to those individuals on a need to know basis only. If CMS determines or has reasonable belief that the User has made an unauthorized disclosure of the data, CMS in its sole discretion may require the User to: (a) Promptly investigate and report to CMS any alleged or actual unauthorized disclosures; (b) promptly resolve any problems identified by the investigation; (c) submit a formal response to any allegation of unauthorized disclosures;

(d) submit a corrective action plan with steps to prevent any future unauthorized disclosures; and (e) return data files to CMS. If CMS determines or has reasonable belief that unauthorized disclosures have taken place; CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

The Privacy Act provides criminal penalties for certain violations. The Act provides that ''[a]ny officer or employee of an agency, who by virtue of his [or her] employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific materials is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000'' (5 U.S.C. 552a (i)(1)). The Act also provides that ''[a]ny person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000 (5 U.S.C. 552a (i)(3)). The agency's contractor and any contractor's employees who are covered by 5 U.S.C. 552a (m) (1) are considered employees of the agency for the purposes of these criminal penalties.

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

Dated: December 4, 2001.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–9002

SYSTEM NAME:

Home Health Agency Outcome and Assessment Information Set (HHA OASIS)

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive

SYSTEM LOCATION:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system of records (SOR) will contain clinical assessment information (OASIS) for all patients receiving the services of a Medicare and/or Medicaid approved HHA, except prepartum and postpartum patients, patients under 18 years of age, and patients receiving other than personal care or health care services; i.e., housekeeping services and chore services. Identifiable information will be maintained in the SOR only for those individuals whose payments come from Medicare or Medicaid.

CATEGORIES OF RECORDS IN THE SYSTEM:

This SOR will contain individual-level demographic and identifying data, as well as clinical status data for patients with the payment sources of Medicare traditional fee for service, Medicaid traditional fee for service, Medicare HMO/managed care or Medicaid HMO/managed care.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Sections 1102(a), 1154, 1861(m), 1861(o), 1861(z), 1863, 1864, 1865, 1866, 1871, 1891, and 1902 of the Social Security Act (the Act) authorize the Administrator of CMS to require HHAs participating in the Medicare and Medicaid programs to complete a standard, valid, patient assessment data set; i.e., the OASIS, as part of their comprehensive assessments and updates when evaluating adult, non-maternity patients as required by section 484.55 of the Conditions of Participation.

PURPOSE(S) OF THE SYSTEM:

The primary purposes of the SOR are to: (1) Study and help ensure the quality of care provided by home health agencies (HHA); (2) aid in administration of the survey and certification of Medicare/Medicaid HHAs; (3) enable regulators to provide HHAs with data for their internal quality improvement activities; (4) support agencies of the state government to determine, evaluate and assess overall effectiveness and quality of HHA services provided in the state; (5) provide for the validation, and refinements of the Medicare Prospective Payment System; (6) aid in the administration of Federal and state HHA programs within the state; and (7) monitor the continuity of care for patients who reside temporarily outside of the state. Information maintained in this system will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) assist another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations; (3) support research, evaluation, or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects; (4) support the functions of Peer Review Organizations (PRO); (5) support the functions of national accrediting organizations; (6) support litigation involving the Agency; (7) support constituent requests made to a Congressional representative; and (8) combat fraud and abuse in certain health care programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF 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 OASIS without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, 65 **Federal Register** (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 this HHS regulation ''Standards for Privacy of Individually Identifiable Health Information.'' We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, or consultants who have been contracted by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system 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, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations 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 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 Peer Review Organizations (PRO) in order to assist the PRO to perform Title XI and Title XVIII functions relating to assessing and improving HHA quality of care.

5. To national accrediting organizations with approval for deeming authority for Medicare requirements for home health services (i.e., the Joint Commission on Accreditation of Healthcare Organizations, or the Community Health Accreditation Program). Information will be released to these organizations only for those facilities that they accredit, and that participate in the Medicare program by virtue of their accreditation (deemed) status.

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 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.

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 programs.

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:

All records are stored on magnetic media.

RETRIEVABILITY:

The Medicare and Medicaid records are retrieved by health insurance claim number, social security number (SSN) or by state assigned Medicaid 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 HHA OASIS system. For computerized records, safeguards have been established in accordance with 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's Information System Security Policy and Program Handbook; and OMB Circular No. A–130 (revised) Appendix III.

RETENTION AND DISPOSAL:

CMS and the repository of the National Archive and Records Administration will retain identifiable OASIS assessment data for a total period not to exceed fifteen (15) years.

SYSTEM MANAGER AND ADDRESS:

Director, Center for Medicaid and State Operations, CMS, 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, health insurance claim number, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), SSN (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay), address, date of birth, and sex.

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:

The Outcome and Assessment Information Set.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 01–31546 Filed 12–26–01; 8:45 am]

BILLING CODE 4120–03–P