Exposure Cohort Petitioning Process Procedures, NIOSH-IREP concerns and model transparency, dose reconstruction workgroup discussion and issues, and Board discussion.

Agenda items are subject to change as priorities dictate.

For Further Information Contact: Larry Elliott, Executive Secretary, ABRWH, NIOSH, CDC, 4676 Columbia Parkway, Cincinnati, Ohio 45226, telephone (513) 841–4498, fax (513) 458–7125.

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 the Centers for Disease Control and Prevention and the Agency for Toxic Substances and Disease Registry.

Dated: June 12, 2002.

John C. Burckhardt,

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

[FR Doc. 02–15273 Filed 6–14–02; 8:45 am]

BILLING CODE 4163–19–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 proposal to modify or alter a 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, ''End Stage Renal Disease (ESRD) Program Management and Medical Information System (PMMIS),'' System No. 09–70–0520. We propose to broaden the scope of this system to include the collection and maintenance of ESRD Core Indicators or Clinical Performance Measures (CPM). Data contained in CPM Data Set are being added to meet statutory requirements and to augment the usefulness of the information for research, quality improvement projects, and policy formulation. We are deleting routine use number 2 authorizing disclosures to organizations deemed qualified to carry out quality assessments; number 5, authorizing disclosures to a contractor; number 6, authorizing disclosures to an agency of a state government; and an unnumbered routine use which authorizes the release of information to the Social Security Administration (SSA).

Routine use number 2 is being deleted because it is not clear what ''organizations'' are being identified and who should receive information referred to in this routine use. We will add a new routine use to accomplish release of information in this system to ESRD Network Organizations and Quality Improvement Organizations (QIO) to carry out quality assessments, medical audits, quality improvement projects, and/or utilization reviews. Disclosures allowed by routine use number 6 and to SSA will be covered by a new routine use to permit release of information to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' Disclosures previously allowed by routine use number 5 will now be covered by proposed routine use 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' intention to disclose individual-specific information contained in this system. The proposed routine uses will be prioritized and reordered according to their proposed usage. We will also update any sections of the system that were affected by the recent reorganization and 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 maintain information on Medicare ESRD beneficiaries, non-Medicare ESRD patients, Medicare approved ESRD hospitals and dialysis facilities, and Department of Veterans Affairs (DVA) patients. The ESRD/PMMIS is used by CMS and the renal community to perform their duties and responsibilities in monitoring the Medicare status, transplant activities, dialysis activities, and Medicare utilization (inpatient and physician/supplier bills) of ESRD patients and their Medicare providers, as well as in calculating the Medicare covered periods of ESRD. Information retrieved from this system of records will also be disclosed to: support regulatory, reimbursement, 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, ESRD Network Organizations and QIOs to implement quality improvement programs, facilitate research on the quality and effectiveness of care provided and payment related projects, support constituent requests made to a congressional representative, support litigation involving the agency, and combat fraud and abuse in certain health benefits programs. We have provided background information about the modified system in the ''Supplementary Information'' section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See ''Effective Dates'' section for comment period.

EFFECTIVE DATES: CMS filed a modified or altered SOR report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on June 1, 2002. In any event, we will not disclose any information under a routine use until 40 days after publication. We may defer implementation of this SOR or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

ADDRESS: 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: Dennis Stricker, Director, Information Support Group, Office of Clinical Standards and Quality, CMS, Room S3–02–01, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is (410) 786–3116. The e-mail address is dstricker@cms.hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Background

The ESRD Program was established in 1972 pursuant to the provisions of 299I, Public Law 92–603. Notice of this system, ESRD/PMMIS was published in a **Federal Register** at 53 FR 62792 (Dec. 29, 1988), 61 FR 6645 (Feb. 21, 1996) (added unnumbered SSA use), 63 FR 38414 (July 16, 1998) (added three fraud and abuse uses), and 65 FR 50552 (Aug. 18, 2000) (deleted one and modified two fraud and abuse uses).

This system contains records on individuals with ESRD who are entitled to receive Medicare benefits or who are treated by DVA health care facilities. Data in this system are used primarily to meet and implement statutory requirements of Public Law (Pub. L.) 92–603, to meet other legislative requirements, support ESRD research, quality improvement projects, and public service programs.

The legislation (§ 299I, Pub. L. 92–603) extended Medicare coverage to individuals with ESRD who require dialysis or transportation to sustain life. This legislation and subsequent regulations also established health and safety standards applicable to providers of ESRD services and required the establishment of ESRD Network Coordinating Councils. The ESRD Networks were established to serve as liaisons between the federal government and the provider of ESRD services. This rule contained an additional requirement of the Omnibus Reconciliation Act of 1986 (Pub. L. 99–509) required that the Secretary establish a national ESRD registry. This registry is called the United States Renal Data System (USRDS). The contract to administer the USRDS was awarded by the National Institutes of Health (NIH) to the Urban Institute on May 1, 1988, for a 5 year period. This registry utilizes data reported by network organizations, transplant centers, and other sources to support the analysis of alternative treatment modes, the evaluation of allocation of resources, the analysis of morbidity and mortality trends and other quality of care indices, and other studies that assist the Congress in evaluating the ESRD program. The second 5 year contract was awarded to the University of Michigan on July 1, 1993. A 12 month extension was then executed for the period of performance of July 1, 1999 to June 30, 1999. A 4 month extension was then granted July 1, 1999. The next 5 year contract was awarded to the Minneapolis Medical Research Foundation on July 1, 1999.

Public Law 95–292 established the ESRD/PMMIS. The PMMIS was created in response to the CMS requirement to provide information on ESRD patients once the above legislation ensured that Medicare would pay for the dialysis treatments and kidney transplants required to sustain a patient's life. The ESRD/PMMIS is a mission critical system to the renal community. The PMMIS was a batch-oriented Model 204 (M204) data system, which later evolved into the Renal Beneficiary and Utilization System (REBUS) M204 on-line system. The acronym PMMIS is retained by a group of data files that have been available to the ESRD community since the batch system was created. The files remain an important product of REBUS operations and retain the PMMIS name for purposes of easy identification by interested users. Thus, the REBUS serves as the primary access mechanism for the PMMIS. We currently have over 1 million individual Master File records in REBUS. Data is supplied to REBUS by approximately 4,637 dialysis and or transplant facilities via the 18 ESRD Networks, and the United Network for Organ Sharing.

Data contained in the Clinical Performance Measures (CPM) Data Set is being added to the ESRD/PMMIS system of records in order to meet statutory requirements and to augment the usefulness of the information for research, quality improvement projects, and policy formulation. CPM data set was developed in response to section 4558(b) of the Balanced Budget Act of 1997, which required the Secretary to develop and implement a method to measure and report the quality of dialysis services under the Medicare program by the year 2000. CPM contains information, in the form of quality measures, on entitled ESRD beneficiaries who receive hemodialysis or peritoneal dialysis treatments. These quality measures are designed based on the National Kidney Foundation-Kidney Disease Outcomes Quality Initiative (K/DOQI) Clinical Practice Guidelines. These quality measures and their respective dimensions presently comprising the CPM are as follows:

- Hemodialysis Adequacy
  - Monthly Measurement of Delivered Hemodialysis Dose
  - Method of Measurement of Delivered Hemodialysis Dose
  - Minimum Delivered Hemodialysis Dose
  - Method of Post-Dialysis Blood Urea Nitrogen (BUN) Sampling
  - Baseline Total Cell Volume Measurement of Dialysis Intended for Reuse
- Peritoneal Dialysis Adequacy
  - Measurement of Total Solute Clearance at Regular Intervals
  - Calculate Weekly Kt/V urea and Creatinine Clearance in a Standard Way
  - Delivered Dose of Peritoneal Dialysis
- Vascular Access
  - Maximizing Placement of Arterial Fistulae
  - Minimizing Use of Catheter as Chronic Dialysis Access
  - Preferred/Non-Preferred location of Hemodialysis Catheters located above the waist
  - Monitoring Arterial Venous Grafts for Stenosis
- Anemia Management
  - Target Hematocrit or hemoglobin for Epoetin Therapy
  - Assessment of Iron Among Anemic Patients or Patients Prescribed Epoetin
  - Maintenance of Iron-stores Target
  - Administration of Supplemental Iron
- Serum Albunin

B. Statutory and Regulatory Basis for System

Authority for maintenance of the system is given under sections 226A, 1875, and 1881 of the Social Security Act (the Act) (Title 42 United States Code (U.S.C.), sections 426–1, 1395ll, and 1395rr).

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system contains information related to individuals with ESRD who receive Medicare benefits or who are treated by DVA health care facilities. The system contains information on both the beneficiary and the provider of services. The system contains beneficiary/patient medical records, claims data, and payment data collected from several non-reimbursement data collection instruments and Medicare bills. The provider of services' name, address, Medicare identification number, types of services provided, certification and or termination date, and ESRD network number.

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 PMMIS information that can be associated with an individual 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.

We will only disclose the minimum personal data necessary to achieve the purpose of PMMIS. 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 to the extent necessary to accomplish the purpose of the disclosure and only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, *e.g.,* monitoring the Medicare status, transplant activities, dialysis activities, and Medicare utilization of ESRD patients.

2. Determines that:

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

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

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

3. Requires the information recipient to:

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

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

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

4.Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the PMMIS without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, or consultants who have been contracted by the Agency to assist in accomplishment of a CMS function relating to the purposes for this SOR and who need to have access to the records in order to assist CMS.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing a CMS function relating to purposes for this SOR.

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

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to:

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

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

c. Determine compliance with the Federal conditions that an ESRD facility must meet in order to participate in Medicare.

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

In addition, disclosure under this routine use shall be used by state agencies pursuant to agreements with the HHS for determining Medicare eligibility, for quality control studies, for determining eligibility of recipients of assistance under titles IV, XVIII, and XIX of the Act, and for the administration of the Medicare program. Data will be released to the state only on those individuals who are patients under the services of a 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 PMMIS information for auditing 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 ESRD Network Organizations and Quality Improvement Organizations in connection with review of claims, or in connection with studies or quality improvements projects or other review activities, conducted pursuant to Part B of Title XI of the Social Security Act and in performing affirmative outreach activities to individuals for the purpose of establishing and maintaining their entitlement to Medicare benefits or health insurance plans.

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

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

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

5. To Members of Congress or to congressional staff members 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.

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 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.

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

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

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

- Database Administrator class owns the database objects; e.g., tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- Quality Indicator Report Generator class has read-only access to all fields and tables;
- Policy Research class has query access to tables, but are not allowed to access confidential patient identification information; and
- Submitter class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards

All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the PMMIS system:

Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information System resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log on—Authentication is performed by the Primary Domain

Controller/Backup Domain Controller of the log-on domain.

• Workstation Names—Workstation naming conventions may be defined and implemented at the Agency level.

• Hours of Operation—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the Agency level.

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

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

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

C. Procedural Safeguards

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

V. Effect of the Modified System On Individual Rights

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. We will only collect the minimum personal data necessary to achieve the purpose of PMMIS. Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure. CMS has assigned a higher level of security clearance for the information in this system to provide added security and protection of data in this system.

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

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

Dated: June 1, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0520

SYSTEM NAME:

End Stage Renal Disease (ESRD) Program Management and Medical Information System (PMMIS), HHS// CMS/OCSQ.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals with ESRD who receive Medicare benefits or who are treated by Department of Veteran Affairs (DVA) health care facilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information on both the beneficiary and the provider of services. The system contains beneficiary/patient medical records, claims data, and payment data collected from several non-reimbursement data collection instruments and Medicare bills. The information contains the provider's name, address, Medicare identification number, types of services provided certification and or termination date, and ESRD network number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under sections 226A, 1875, and 1881 of the Social Security Act (the Act)(Title 42 United States Code (U.S.C.) 426–1, 1395ii, and 1395rr).

PURPOSE(S):

The primary purpose of the system of records is to maintain information on Medicare ESRD beneficiaries, non-Medicare ESRD patients, Medicare approved ESRD hospitals and dialysis facilities, and DVA patients. The ESRD/PMMIS is used by CMS and the renal community to perform their duties and responsibilities in monitoring the Medicare status, transplant activities, dialysis activities, and Medicare utilization (inpatient and physician/supplier bills) of ESRD patients and their Medicare providers, as well as in calculating the Medicare covered periods of ESRD. Information retrieved from this system of records will also be disclosed to: support regulatory, reimbursement, 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, ESRD Network organizations and QIOs to implement quality improvement programs, facilitate research on the quality and effectiveness of care provided and payment related projects, support constituent requests made to a congressional representative, support litigation involving the agency, and combat fraud and abuse in certain health benefits programs.

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

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

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 (12–28–00), as amended by 66 FR 12434 (2–26–01)). Disclosures of Protected Health Information authorized

by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.'' We are proposing to establish or modify the following routine use disclosures of information maintained in the system:

1. To Agency contractors, or consultants who have been contracted by the Agency to assist in accomplishment of a CMS function relating to the purposes for this SOR and who need to have access to the records in order to assist CMS.

2. To another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to:

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

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

c. Determine compliance with the Federal conditions that an ESRD facility must meet in order to participate in Medicare.

3. To ESRD Network Organizations and Quality Improvement Organizations in connection with review of claims, or in connection with quality improvements projects, 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.

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

5. To Members of Congress or to congressional staff members 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 FIs and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

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:

All records are stored on magnetic media or hard paper copy.

RETRIEVABILITY:

All Medicare records are accessible by health insurance claim number, individual's name, or the provider 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 PMMIS 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 indefinitely.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Information Support Group, Office of Clinical Standards and Quality, CMS, Room S3–02–01, 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, provider identification number, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

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

CONTESTING RECORD PROCEDURES:

The subject individual should contact the 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 data contained in these records are obtained from Medicare ESRD medical evidence reports, kidney transplant reports, ESRD beneficiary reimbursement method selection forms, ESRD death notification forms, Medicare bills, CMS Medicare Master files, ESRD facility surveys, ESRD facility certification notices, and the Medicare/Medicaid Automated Certification System (MMACS).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

Appendix A

1. ESRD Network of New England, Incorporated, Post Office Box 9484, New Haven, Connecticut 06534.
2. ESRD Network of New York, Incorporated, 1249 Fifth Avenue, A–419, New York, New York 10029.
3. Trans-Atlantic Renal Council, Cranbury Plaza, 2525 Route 130-Building C, Cranbury, New Jersey 08512–9595.
4. ESRD Network Organization Number 4, 200 Lothrop Street, Pittsburgh, Pennsylvania 15213–2582.
5. Mid-Atlantic Renal Coalition, 1527 Huguenot Road, Midlothian, Virginia 23113.
6. Southeastern Kidney Council, Incorporated, 1000 Saint Albans Drive, Suite 270, Raleigh, North Carolina 27609.
7. ESRD Network of Florida, Incorporated, One Davis Boulevard, Suite 304, Tampa, Florida 33606.
8. Network 8, Incorporated, Post Office Box 55868, Jackson, Mississippi 39296–5868.
9 & 10. The Renal Network, Incorporated, 911 East 86th Street, Suite 202, Indianapolis, Indiana 46240.
11. Renal Network of the Upper Midwest, 970 Raymond Avenue #205, Saint Paul, Minnesota 55114.
12. ESRD Network Number 12, 7509 NW T Tiffany Spring Parkway, Suite 105, Kansas City, Missouri 64153.
13. ESRD Network Organization Number 13, 6600 North Meridan Avenue, Suite 155, Oklahoma City, Oklahoma 73116–1411.
14. ESRD Network of Texas, Incorporated, 14114 Dallas Parkway, Suite 660, Dallas, Texas 75240–4349.
15. Intermountain ESRD Network, Incorporated, 1301 Pennsylvania Street, Suite 220, Denver, Colorado 80203–5012.
16. Northwest Renal Network, 4702 42nd Avenue, Seattle, Washington 98116.
17. TransPacific Renal Network, 25 Mitchell Boulevard, Suite 7, San Rafael, California 94903.
18. Southern California Renal Disease Council, 6255 Sunset Boulevard, Suite 2211, Los Angeles, California 90082.

[FR Doc. 02–15007 Filed 6–14–02; 8:45 am]
BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Submission for OMB Review; Comment Request

Title: Temporary Assistance for Needy Families (TANF) State Plan Guidance.

OMB No.: 0970–0145.

Description: The State plan is a mandatory statement submitted to the Secretary of the Department of Health and Human Services by the State. It consists of an outline of how the State's TANF program will be administered and operated and certain required certifications by the State's Chief Administrative Officer. Its submittal triggers the State's family assistance grant funding and it is used to provide the public with information about the program. If a State makes changes in its program, it must submit a State plan amendment.

Respondents: States.

Annual Burden Estimates:

Instrument	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
State TANF plan	54	1	30	1,620
Title Amendments	54	1	3	162

Estimated Total Annual Burden Hours: 1782

Additional Information: Copies of the proposed collection can be obtained by writing to the Administration for Children and Families, Office of Information Services, 370 L'Enfant Promenade, SW., Washington, DC 20447, Attn: ACF Reports Clearance Officer.

OMB Comment: OMB is required to make a decision concerning the collection of information between 30 and 60 days after publication of this document in the **Federal Register**. Therefore, a comment is best assured of having its full effect if OMB receives it within 30 days of pubublication. Written comments and recommendations for the proposed information collection should be sent directly to the following: Office of Management and Budget, Paperwork Reduction Project, 725 17th Street, NW., Washington, DC 20503, Attn: Desk Officer for ACF.

Dated: May 28, 2002.

Bob Sargis,

Reports Clearance Officer.

[FR Doc. 02–15115 Filed 6–14–02; 8:45 am]
BILLING CODE 4184–01–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

Request for Nominations for Voting Members on Public Advisory Committees; Veterinary Medicine Advisory Committee; Extension of Nomination Period

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice; extension of nomination period.

SUMMARY: The Food and Drug Administration (FDA) is extending the nomination period for voting members to serve on the Veterinary Medicine Advisory Committee (VMAC) in one of the following specialty areas: Pharmacology, Minor Species/Minor Use Veterinary Medicine, and pathology. Nominations for the VMAC chairperson are also being solicited. This request for nominations was announced in the **Federal Register** of May 13, 2002 (67 FR 32055). FDA has been asked to extend the nominations period to allow additional time for the submission of nominations.

DATES: Nominations should be received by June 30, 2002.

ADDRESSES: All nominations for representatives should be sent to Aleta Sindelar (see **FOR FURTHER INFORMATION CONTACT**).

FOR FURTHER INFORMATION CONTACT: Aleta Sindelar, Center for Veterinary Medicine, Food and Drug Administration, 7519 Standish Pl., Rockville, MD 20855, 301–827–4515, e-mail: asindela@cvm.fda.gov.

Dated: June 6, 2002.

William K. Hubbard,

Senior Associate Commissioner for Policy, Planning, and Legislation.

[FR Doc. 02–15111 Filed 6–14–02; 8:45 am]
BILLING CODE 4160–01–S