Dated: June 11, 2003.

Thomas A. Bartenfeld,

Acting Associate Director for Policy, Planning and Evaluation, Centers for Disease Control and Prevention.

[FR Doc. 03–15216 Filed 6–16–03; 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 New System

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

ACTION: Notice of New System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system of records, called the ''MLN Registration and Product Ordering System (MLNR-POS),'' HHS/CMS/CMM No. 09–70–0542. The primary purpose of the system of records is to provide CMS with greater efficiency in MLNR-POS product fulfillment and improve management of MLNR-POS educational product inventory. This system will also provide CMS with an automated registration system that will allow health care providers to register for CMS educational programs and order CMS educational products. If in the event that CMS becomes an accredited provider of continuing education credits, this system will provide CMS with the ability to track awarded continuing education credits as required by the accrediting organizations.

Information retrieved from this system of records will be used to support regulatory, reimbursement, and policy functions performed within the agency or by a contractor or consultant; support constituent requests made to a Congressional representative; and support litigation involving the agency.

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

DATES: CMS filed a new system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on May 23, 2003. In any event, we will not disclose any information under a routine use until forty (40) calendar days after publication. We may defer implementation of this system of records 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 Privacy Compliance Data Development (DPCDD), 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 9:00 a.m.-3:00 p.m., eastern time zone.

FOR FURTHER INFORMATION CONTACT: Mary Case, Division of Provider Information Planning and Development (DPIPD), CMS, Mail Stop C4–10–07, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

SUPPLEMENTARY INFORMATION:

I. Description of the New System of Records

A. Statutory and Regulatory Basis for System of Records

Title IV of the Benefits Improvement Protection Act of 2000 (Pub. L. 106–554, Appendix F)

Title IV of the Balanced Budget Act of 1997 Sections 1816(a) and 1842 (a) (3) of the Social Security Act

B. Background

Studies have shown that providers are very interested in obtaining information that will help them improve their billing procedures and improve patient care. These studies have also shown that providers are limited on the amount of time they can spend away from their practice to attend conferences and sort though the multitude of correspondence that they receive on a daily basis. Distance learning is an educational avenue that physicians find an appealing alternative. Studies have shown that health care providers better utilize educational products that provide continuing education credits.

This registration and product ordering system will allow health care providers to register for computer/web-based training courses, satellite broadcasts and train-the-trainer sessions. The system will also allow learners to order provider educational materials.

CMS is considering applying to become an accredited provider of continuing education. If accredited, CMS will use this system to track continuing education credit information as required by the accrediting organizations.

According to Donna S. Queeney in the American Society for Training and Development Handbook, Fourth Edition, ''continuing professional education often is used as a component of credentialing with the intention that it will help practitioners keep knowledge, skills and performance abilities current.'' Ms. Queeney also states ''required continuing education must be accessible to practitioners regardless of their work schedules, geographic locations, or other mitigating factors. The solo practitioner in a rural area needs ready access to continuing education just as much as the group practitioner in a major metropolitan area.''

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The MLNR-POS database will collect and store the health care provider's first and last name, mailing address, provider type, facility type, telephone number, fax number and email address. If CMS becomes an accredited provider of continuing education credits, this system may also contain social security number, provider number, UPIN number or contractor ID number.

This information will be used by CMS and CMS contractors to confirm registration and report aggregate data and allow health care providers to retrieve their own educational information.

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 MLNR-POS 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. Identifiable data includes individual records with MLNR-POS information and identifiers. Non-identifiable data includes individual records with MLNR-POS information and masked identifiers or MLNR-POS information with identifiers stripped out of the file.

CMS will only disclose the minimum personal data necessary to achieve the purpose of the MLNR-POS. 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:

1. Determines that the use or disclosure is consistent with the reason that the data are being collected; *e.g.*, tracking, reporting and accounting the disclosures made from all CMS systems of records as permitted by the Privacy Act and HIPAA.

2. Determines that:

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

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

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

3. Requires the information recipient to:

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

b. Remove or destroy at the earliest time all individually, identifiable information; and

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

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities That 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 MLNR-POS 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. CMS proposes to establish the following routine use disclosures of information maintained in the system:

1. To agency contractors, or consultants that have been contracted by the agency to assist in the performance of a service related to this system of records and that need to have access to the records in order to perform the activity.

CMS contemplates 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 agency business functions relating to purposes for this system of records.

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

2. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional Office made at the written request of the constituent about whom the record is maintained.

Individuals sometimes request the help of a Member of Congress in resolving 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.

3. 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 agreedto 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. A determination would be made in each instance that, under the circumstances involved, the purposes served by the use of the information in the particular litigation is compatible with a purpose for which CMS collects the information.

B. Additional Provisions Affecting Routine Use Disclosures

In addition, CMS 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 System of Records contains Protected Health Information as defined by the Department of Health and Human Services' regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR Parts 160 and 164, 65 **Federal Register** 82462 as amended by 66 **Federal Register** 12434). 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.''

IV. Safeguards

The MLNR–POS will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and 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 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. Records are used in a designated work area and system location is attended at all times during working hours.

To ensure security of the data, the proper level of class user is assigned for each individual user 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.

B. Physical Safeguards

All server sites will implement 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 CMS system:

Access to all servers is to be 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 is to require 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, which 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 Systems (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-on—Authentication is to be 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 to be determined and implemented at the agency level.
- Inactivity Lockout—Access to the NT workstation is to be automatically locked after a specified period of inactivity.
- Warnings—Legal notices and security warnings are to be displayed on all servers and workstations.
- Remote Access Security—Windows NT Remote Access Service (RAS) security handles resource access control. Access to NT resources is to be 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. These include, but are not limited to: the Privacy Act of 1974; the Computer Security Act of 1987; OMB Circular A–130, revised; Information Resource Management Circular #10; HHS AIS Security Program; the CMS Information Systems Security Policy, Standards, and Guidelines Handbook; and other CMS systems security policies. 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. Effects of the New 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. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CMS will monitor the collection and reporting of MLNR–POS data. MLNR–POS information is submitted to CMS through standard systems. CMS will use a variety of onsite and offsite edits and audits to increase the accuracy of MLNR–POS 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 of patients whose data are maintained in the system. 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 maintaining this system of records.

Dated: May 23, 2003.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0542

SYSTEM NAME:

MLN Registration and Product Ordering System, (MLNR–POS), HHS/CMS/CMM.

SECURITY CLASSIFICATION:

Level 3, Privacy Act Sensitive.

SYSTEM LOCATION:

HCFA 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:

This system will contain the health care provider's first and last name, mailing address, provider type, facility type, telephone number, fax numbers and e-mail address. The data submission by the health care provider is voluntary. This system may collect social security number, provider number, UPIN number or contractor ID number.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system will contain the health care provider's first and last name, mailing address, provider type, facility type, telephone number, fax numbers and e-mail address. The data submission by the health care provider is voluntary. This system may collect social security number, provider number, UPIN number or contractor ID number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title IV of the Benefits Improvement Protection Act of 2000 (Pub. L. 106–554, Appendix F) Title IV of the Balanced Budget Act of 1997 Sections 1816(a) and 1842(a)(3) of the Social Security Act

PURPOSE(S):

The primary purpose of the system of records is to provide CMS with greater efficiency in MLNR–POS product fulfillment and improve management of MLNR–POS educational product inventory. This system will also provide CMS with an automated registration system that will allow health care providers to register for CMS educational programs and order CMS educational products. If in the event that CMS becomes an accredited provider of continuing education credits, this system will provide CMS with the ability to track awarded continuing education credits as required by the accrediting organizations.

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 MLNR–POS Registration and Product Ordering System 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, CMS 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). Be advised, this System of Records contains Protected Health Information as defined by the Department of Health and Human Services' (HHS) regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 8462 as amended by 66 FR 12434). 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.''

1. To agency contractors, or consultants that have been contracted by the agency to assist in the performance of a service related to this system of records and that need to have access to the records in order to perform the activity.

2. 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.

3. 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 agreedto 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.

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

STORAGE:

Records are stored on paper and magnetic media.

RETRIEVABILITY:

The health care provider, through their self-identified user ID and password can retrieve their own records. Those with database administrative access may also access the database information.

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 CMS 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 Information Systems Security, Standards Guidelines Handbook and OMB Circular No. A–130 (revised) Appendix III.

RETENTION AND DISPOSAL:

Records are disposed of in accordance with established CMS, Privacy Act and HIPAA retention guidelines. CMS will conduct periodic reviews to determine if these records are historical and should be placed in permanent files after established retention periods and administrative needs of CMS have elapsed.

The records are maintained online in the system for 8 years. After an 8-year period, the records are transferred to an inactive file and destroyed 2 months later.

Note: The Department of Justice issued a directive in 1992 prohibiting the destruction of Medicare claims/administrative records. Therefore, all Medicare claims-related/ administrative data will be retained until the freeze is lifted.''

SYSTEM MANAGER(S) AND ADDRESS:

Director, Provider Communications Group (PCG), Center for Medicare Management, CMS, Mail Stop S1–05–06, 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, the subject individual's name (woman's maiden name, if applicable), social security number (SSN) (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay), address, date of correspondence and control number.

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:

Data submission is voluntary and is self reported by the health care provider.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 03–15120 Filed 6–16–03; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 2003D–0229]

Draft Guidance for Industry on Continuous Marketing Applications: Pilot 2—Scientific Feedback and Interactions During Development of Fast Track Products Under the Prescription Drug User Fee Act

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA) is announcing the availability of a draft guidance for industry entitled ''Continuous Marketing Applications: Pilot 2—Scientific Feedback and Interactions During Development of Fast Track Products Under PDUFA.'' This guidance discusses how the agency will implement a pilot program for frequent scientific feedback and interactions between FDA and applicants during the investigational phase of the development of certain Fast Track drug and biological products. Applicants are being asked to apply to participate in the Pilot 2 program.

DATES: Submit written comments on the draft guidance by August 1, 2003. General comments on agency guidance documents are welcome at any time. Submit written or electronic comments on the collection of information by August 15, 2003.

ADDRESSES: Submit written requests for single copies of the guidance to the Division of Drug Information (HFD–240), Center for Drug Evaluation and Research (CDER), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857; or the Office of Communications, Training, and Manufacturers Assistance (HFM–40), Center for Biologics Evaluation and Research (CBER), 1401 Rockville Pike, Rockville, MD 20852–1448. Send one self-addressed adhesive label to assist either office in processing your request. *See* the **SUPPLEMENTARY INFORMATION** section for electronic access to the guidances.

Submit written comments on the draft guidance and on the collection of information to the Division of Dockets Management (HFA–305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments on the draft guidance and the collection of information to *http://www.fda.gov/dockets/ecomments*.

FOR FURTHER INFORMATION CONTACT: John Jenkins, Center for Drug Evaluation and Research (HFD–020), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301–594–3937, or

Robert A. Yetter, Center for Biologics Evaluation and Research (HFM–25), Food and Drug Administration, 1401 Rockville Pike, Rockville, MD 20852, 301–827–0373.

SUPPLEMENTARY INFORMATION:

I. Description of the Guidance

FDA is announcing the availability of a draft guidance for industry entitled ''Continuous Marketing Applications: Pilot 2—Scientific Feedback and Interactions During Development of Fast Track Products Under PDUFA.'' In conjunction with the June 2002 reauthorization of the Prescription Drug User Fee Act of 1992 (PDUFA), FDA agreed to meet specific performance goals (PDUFA Goals). The PDUFA Goals include two pilot programs to explore the continuous marketing application (CMA) concept. The CMA concept builds on the current practice of interaction between FDA and applicants during drug development and application review and proposes opportunities for improvement.

Under this CMA pilot program, Pilot 2, certain drug and biologic products that have been designated as Fast Track (i.e., products intended to treat a serious and/or life-threatening disease for which there is an unmet medical need) are eligible to participate in Pilot 2. Pilot 2 is an exploratory program that will allow FDA to evaluate the impact of frequent scientific feedback and interactions with applicants during the investigational new drug application (IND) phase. Under the pilot program, a maximum of one Fast Track product per review division in CDER and CBER will be selected to participate. This guidance provides information regarding the selection of participant applications for Pilot 2, the formation of agreements between FDA and applicants on the IND communication process, and other procedural aspects of Pilot 2. The FDA will begin accepting applications for participation in Pilot 2 on October 1, 2003.

This draft guidance is being issued consistent with FDA's good guidance practices regulation (21 CFR 10.115). The draft guidance, when finalized, will represent the agency's current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statutes and regulations.

II. Comments

Interested persons may submit to the Division of Dockets Management (*see* **ADDRESSES**) written or electronic comments on the draft guidance and the information collection. Two copies of mailed comments are to be submitted, except that individuals may submit one copy. Comments are to be identified with the docket number found in brackets in the heading of this document. The draft guidance and received comments are available for public examination in the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday.

III. The Paperwork Reduction Act of 1995

Under the Paperwork Reduction Act (the PRA) (44 U.S.C. 3501–3520), Federal agencies must obtain approval from the Office of Management and Budget (OMB) for each collection of information they conduct or sponsor. Section 3506(c)(2)(A) of the PRA (44 U.S.C. 3506(c)(2)(A)) requires Federal agencies to provide a 60-day notice in the **Federal Register** concerning each proposed collection of information before submitting the collection to OMB for approval. To comply with this requirement, FDA is publishing notice of the proposed collection of information set forth in this document.

With respect to the following collection of information, FDA invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of FDA's functions, including whether the information will have practical utility; (2) the accuracy of FDA's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility, and clarity of the information to be