both relevant and necessary to the litigation.

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 program.

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:

Records are stored on both tape cartridges (magnetic storage media) and in a DB2 relational database management environment (DASD data storage media).

RETRIEVABILITY:

Information is most frequently retrieved by HIC, provider number (facility, physician, supplier IDs), service dates, type of bill, Medicare status code, diagnoses, procedure codes, and beneficiary state code.

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 NCH 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, Appendix III.

RETENTION AND DISPOSAL:

Records are maintained with identifiers for all transactions after they are entered into the system for a period of 20 years. Records are housed in both active and archival files.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Enrollment and Utilization Data Development, Enterprise Databases Group, Office of Information Services, CMS, Room N3–16–28, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of notification, the subject individual should write to the system manager who will require the system name, and the retrieval selection criteria (e.g., HIC, facility ID, physician/supplier number, service dates, type of bill, etc.).

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:

Fee-for-Service (FFS) billing and utilization information contained in this records system is obtained from the Common Working File, System No. 09–70–0526. Medicare+Choice (M+C) organization utilization information to be contained in this records system will be obtained from a single front-end processor that will function as both a Fiscal Intermediary (System No. 09–70–0503) and Carrier (System No. 09–70–0501).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–22741 Filed 9–5–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of 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 ''Correspondence Tracking Management System (CTMS),'' HHS/CMS/OSORA No. 09–70–3005. The CMTS replaces the Correspondence and Assignment Tracking and Control System (CATCS), System No. 09–70–9001 that was deleted from CMS' database inventory through a published notice in the **Federal Register**. The primary purpose of the system of records is to aid CMS in tracking incoming correspondence about CMS programs from the Office of the Secretary, Medicare beneficiaries and Medicaid recipients. In addition, it will track all correspondence from the public, other government agencies, contractors, and members of the Congress. 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.

EFFECTIVE 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 August 20, 2002. 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 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 time zone.

FOR FURTHER INFORMATION CONTACT: Chris Worrall, Division of Correspondence Control, Office of Communications and Operations Support, CMS, 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

42 CFR 401.101–401.148 and 1106(a) of the Social Security Act, 42 U.S.C. 1306(a).

B. Background

The CMTS is being established to replace the Correspondence and Assignment Tracking and Control System (CATCS), System No. 09–70–9001 that was deleted from CMS' database inventory through a published notice in the **Federal Register**.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The CMTS includes the following information: name and address of correspondent(s); subject of request; Centers/Office to which case is assigned, correspondence control number, date of initial entry and any subsequent updating, location of case, due date, type(s) of information requested, any cross reference, incoming correspondence, response and if provided in the correspondence, information about a beneficiary (*e.g.*, name, address, Social Security 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 CMTS 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 CMTS information and identifiers. Non-identifiable data includes individual records with CMTS information and masked identifiers or CMTS information with identifiers stripped out of the file.

CMS will only disclose the minimum personal data necessary to achieve the purpose of the CMTS. 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.*, track, control, and respond to correspondence from the public, other government agencies, contractors, and members of the Congress.

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 CMTS 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 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. 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 FR 82462 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.''

IV. Safeguards

The CMTS system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act 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. 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 CMTS data. CMTS 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 CMTS 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.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–3005

SYSTEM NAME:

Correspondence Tracking Management System, (CMTS).

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:

The system of records will contain data on any correspondent whose letter is sent to CMS and on individuals referenced in such correspondence (*e.g.*, beneficiaries, the public, other government agencies, contractors, and members of the Congress.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains incoming correspondence, responses to correspondence and information CMS uses to track correspondence, and *e.g.* CMTS control number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 CFR 401.101–401.148 and sec 1106(a) of the Social Security Act, 42 U.S.C. 1306(a).

PURPOSE(S):

The primary purpose of the system of records is to aid CMS in tracking incoming correspondence about CMS programs from the Office of the Secretary, Medicare beneficiaries and Medicaid recipients. In addition, it will track all correspondence from the public, other government agencies, contractors, and members of the Congress. 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.

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 CMTS 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 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.

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

STORAGE:

All records are stored on magnetic media.

RETRIEVABILITY:

Name of correspondent, name of individual referenced in the correspondence, or correspondence control number retrieves the records.

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:

The records are maintained on-line in the system for 2 years. After a 2-year period, records are transferred to an archive file and destroyed three years later.

Due to a freeze imposed by the Department of Justice in 1992, correspondence documenting/supporting a specific claim, reconsideration, appeal or similar case will be maintained until further notice. Once the freeze is lifted, destroy 6 years and 3 months after final payment/resolution.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Correspondence Control, Office of Communications and Operations Support, Health Care Financing Administration, 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.

RECORD ACCESS PROCEDURES:

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:

Incoming correspondence and responses to such correspondence.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–22742 Filed 9–5–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 01P–0343]

Orthopedic Devices; Denial of Request for Change in Classification of Hip Joint Metal/Metal Semi-Constrained, With a Cemented Acetabular Component, Prosthesis and Hip Joint Metal/Metal Semi-Constrained, With an Uncemented Acetabular Component, Prosthesis

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice; denial of petition.

SUMMARY: The Food and Drug Administration (FDA) is denying the petition submitted by the Orthopedic Surgical Manufacturers Association (OSMA) to reclassify the hip joint metal/metal semi-constrained prosthesis with a cemented acetabular component and the hip joint metal/metal semi-constrained prosthesis with an uncemented acetabular component from class III (premarket approval) into class II (special controls). The agency is denying the petition because OSMA failed to provide any new information to establish that special controls would provide reasonable assurance of the safety and effectiveness of the devices. The agency is also publishing the recommendation of FDA's Orthopedic and Rehabilitation Devices Panel (the Panel) concerning the petition. This action is being taken under the Federal Food, Drug, and Cosmetic Act (the act), as amended by the Medical Device Amendments of 1976 (the 1976 amendments), the Safe Medical Devices Act of 1990 (SMDA), and the Food and Drug Administration Modernization Act of 1997 (FDAMA).

FOR FURTHER INFORMATION CONTACT: Glenn A. Stiegman, Center for Devices and Radiological Health (HFZ–410), Food and Drug Administration, 9200 Corporate Blvd., Rockville, MD 20850, 301–594–2036.

SUPPLEMENTARY INFORMATION:

I. Classification and Reclassification of Devices Under the Amendments

The act (21 U.S.C. 301 *et seq.*), as amended by the 1976 amendments (Public Law 94–295), SMDA (Public Law 101–629) and FDAMA (Public Law 105–115), established a comprehensive system for the regulation of medical devices intended for human use. Section 513 of the act (21 U.S.C. 360c) established three categories (classes) of devices, depending on the regulatory controls needed to provide reasonable assurance of their safety and effectiveness. The three categories of devices are class I (general controls), class II (special controls), and class III (premarket approval). Except as provided in section 520(c) of the act (21 U.S.C. 360j(c)), FDA may not use confidential information concerning a device's safety and effectiveness as a basis for reclassification of the device from class III into class II or class I.

Under section 513 of the act, devices that were in commercial distribution before May 28, 1976 (the date of enactment of the amendments), generally referred to as preamendments devices, are classified after FDA has: (1) Received a recommendation from a device classification panel (an FDA advisory committee); (2) published the panel's recommendation for comment, along with a proposed regulation classifying the device; and (3) published a final regulation classifying the device. FDA has classified most preamendment devices under these procedures.

Devices that were not in commercial distribution prior to May 28, 1976, generally referred to as postamendments devices, are classified automatically by statute (section 513(f) of the act) into class III without any FDA rulemaking process. Those devices remain in class III and require premarket approval, unless and until: (1) The device is reclassified into class I or II; (2) FDA issues an order classifying the device into class I or II in accordance with new section 513(f)(2) of the act, as amended by FDAMA; or (3) FDA issues an order finding the device to be substantially equivalent, under section 513(i) of the act, to a predicate device that does not require premarket approval. The agency determines whether new devices are substantially equivalent to previously marketed devices by means of premarket notification procedures in