Board's formal interpretations for loans purchased by a bank from an affiliate.

5. Proposed 2003 fees for priced services and electronic connections.

6. Any items carried forward from a previously announced meeting.

Note: This meeting will be recorded for the benefit of those unable to attend. Cassettes will be available for listening in the Board's Freedom of Information Office and copies may be ordered for $6 per cassette by calling 202–452–3684 or by writing to: Freedom of Information Office, Board of Governors of the Federal Reserve System, Washington, DC 20551.

FOR FURTHER INFORMATION CONTACT: Michelle A. Smith, Assistant to the Board; 202–452–2955.

SUPPLEMENTARY INFORMATION: You may call 202–452–3206 for a recorded announcement of this meeting; or you may contact the Board's Web site at *http://www.federalreserve.gov* for an electronic announcement. (The Web site also includes procedural and other information about the open meeting.)

Dated: October 24, 2002.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 02–27524 Filed 10–24–02; 3:07 pm]

BILLING CODE 6210–01–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 modified or altered system of records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to modify or alter a SOR, ''CMS Utilization Review Investigatory Files, System No. 09–70–0527.'' We propose to change the name of this system to ''CMS Fraud Investigation Database (FID),'' to more accurately reflect the increase in scope proposed by this modification. We propose to broaden the scope of responsibility and activities covered by this system to include activities related to fraud and abuse in all health care programs administered by CMS. We are deleting routine uses number 1 pertaining to Department of Justice (DOJ) for consideration of criminal prosecution or civil action, number 2 pertaining to state or local licensing authorities (including state medical review boards), professional review organizations, peer review groups, medical consultants, or other professional associations for possible administrative action, number 3 pertaining to * * * officers and employees of state governments * * * Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) * * * as well as states attorneys * * *, number 4 pertaining to * * * third parties for the purpose of establishing or negating a violation, number 5 pertaining to * * * cases involving fraudulent tax returns or forger of Medicare checks to the Treasury Department, postal authorities, or to appropriate law enforcement authorities, and an unnumbered routine use authorizing disclosure to the Social Security Administration (SSA).

Disclosures of the data allowed in routine uses number 1, 2, 3, 4, 5, and to the SSA will be accomplished by a new routine use ''to combat fraud and abuse in certain health benefits programs'' and will be numbered as routine use number 5. We propose a new routine use number 1 specifically for the release of information in the system to a contractor or consultant who need to have access to the records in order to assist CMS. We propose a new routine use number 4 specifically for the release of information in the system to a contractor that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program to combat fraud and abuse. We propose to modify the language of routine uses number 6 and number 7 to clarify the circumstances for disclosure under these routine uses and change the numbers of these routine uses to number 2 and number 3.

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.'' The routine uses will then be prioritized and reordered according to their proposed usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization and to update language in the administrative sections to correspond with language used in other CMS SOR.

The primary purpose of this SOR is to identify if a violation(s) of a provision of the Social Security Act (the Act) or a related penal or civil provision of the United States Code (U.S.C.) related to Medicare (Title XVIII), Medicaid (Title XIX), HMO/Managed Care (Title XX), and Children's Health Insurance Program (Title XXI) have been committed, determine if HHS has made a proper payment as prescribed under applicable sections of the Act and whether these programs have been abused, coordinate investigations related to Medicare, Medicaid, HMO/Managed Care, and Children's Health Insurance Program, and prevent duplications, and provide case file material to the HHS Office of Inspector General when a case is referred for fraud investigation. Information retrieved from this SOR will also be disclosed to: (1) Support regulatory and policy functions performed within the Agency or by a contractor or consultant; (2) support constituent requests made to congressional representatives; (3) support litigation involving the Agency related to this system; and (4) combat fraud and abuse in certain health care programs. We have provided background information about the modified system in the ''Supplementary Information'' section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See ''Effective Dates'' section for comment period.

EFFECTIVE DATES: CMS filed a modified or altered system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on September 9, 2002. To ensure that all parties have adequate time in which to comment, the modified or altered SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the congress, whichever is later, unless CMS receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution, Office of Information Services, 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: Mark Koepke, Division of Program Integrity Operations, Program Integrity Group, Office of Financial Management, CMS, Mail-stop C3–02–16, 7500 Security Boulevard, Baltimore,

Maryland 21244–1850. The telephone number is 410–786–0524.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Statutory and Regulatory Basis for SOR

In 1988, CMS established a SOR the authority of sections 205, 1106, 1107, 1815, 1816, 1833, 1842, 1872, 1874, 1876, 1877, and 1902 of the Act, United States Code (U.S.C.) sections 405, 1306, 1307, 1395g, 1395h, 1395l, 1395u, 1395ii, 1395kk, 1395mm, 1395nn, and 1396a). Notice of this system, ''CMS Utilization Review Investigatory Files, System No. 09–70–0527,'' was published in the **Federal Register** at 53 FR 52792, (Dec. 29, 1988), an unnumbered routine use was added for SSA at 61 FR 6645 (Feb. 21, 1996), three new fraud and abuse routine uses were added at 63 FR 38414 (July 16, 1998), and then at 65 FR 50552 (Aug. 18, 2000), two of the fraud and abuse routine uses were revised and a third deleted.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system contains the name, work address, work phone number, social security number, Unique Provider Identification Number (UPIN), and other identifying demographics of individuals alleged to have violated provision of the Act related to Medicare, Medicaid, HMO/Managed Care, and Children's Health Insurance Program or other criminal/civil statutes as they pertain to The Act programs where substantial basis for criminal/civil prosecution exist, defendants in criminal prosecution cases, or persons alleged to have abused the programs. The last category of individuals would, for example, include persons alleged to have rendered unnecessary services to Medicare beneficiaries or Medicaid recipients, over utilized services, or engaged in improper billing.

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, which 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 FID 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 FID information and identifiers. Non-identifiable data includes individual records with FID information and masked identifiers or FID information with identifiers stripped out of the file.

We will only collect the minimum personal data necessary to achieve the purpose of FID. 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 system of records will be approved only for the minimum information necessary to accomplish the purpose of the disclosure only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, *e.g.*, disclosure of individual-specific information for the purposes of combating fraud and abuse in a health benefits program funded in whole or in part by Federal funds.

2. Determines:

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

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

3. Requires the information recipient to:

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

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

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

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the FID 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 engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system of records and who need to have access to the records in order to assist CMS.

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

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

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

Beneficiaries and other individuals often 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.

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.

4. To a CMS contractor (including, but not limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

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

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

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

A. 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 FID system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, the Clinger-Cohen Act of 1996, and OMB Circular A–130, appendix III, ''Security of Federal Automated Information Resources.'' CMS has prepared a comprehensive system security plan as required by the Office and Management and Budget (OMB) Circular A–130, appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems.'' Paragraphs A–C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

Authorized users: Personnel having access to the system have been trained in Privacy Act 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 or workstation and the system location is attended at all times during working hours.

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

- *Database Administrator* class owns the database objects, *e.g.*, tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- *Quality Control Administrator* class has read and write access to key fields in the database;
- *Quality Indicator Report Generator* class has read-only access to all fields and tables;
- *Policy Research* class has query access to tables, but are not allowed to access confidential personal 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 FID system: Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information System resources caused by fire, electricity, water, and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-ons—Authentication is performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.
- Workstation Names—Workstation naming conventions may be defined and implemented at the Agency level.
- Hours of Operation—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are

determined and implemented at the Agency level.

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

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

• Remote Access Security (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. 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 Automated Information Systems Security Program, the CMS Information Systems Security Policy and Program 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. 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. 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 FID data. FID information on individuals is completed by contractor personnel and submitted to CMS through standard systems located at different locations. CMS will utilize a variety of onsite and offsite edits and audits to increase the accuracy of FID data.

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

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

Dated: September 9, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

System No. 09–70–0527

SYSTEM NAME:

Centers for Medicare & Medicaid Services (CMS) Fraud Investigation Database (FID), HHS/CMS/OFM.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitivity.

SYSTEM LOCATION:

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850. Information in this system is also maintained at various remote locations listed in appendix ''A.''

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals alleged to have violated provision of the Act related to Medicare (Title XVIII), Medicaid (Title XIV), HMO/Managed Care (Title XX), and Children's Health Insurance Program (Title XXI) or other criminal/civil statutes as they pertain to the Act programs where substantial basis for criminal/civil prosecution exist, defendants in criminal prosecution cases, or persons alleged to have abused the programs.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains the name, work address, work phone number, social security number, Unique Provider Identification Number (UPIN), and other identifying demographics of individuals alleged to have violated provision of the Act or persons alleged to have abused Medicare and/or Medicaid programs.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system was established under the authority of sections 205, 1106, 1107, 1815, 1816, 1833, 1842, 1872, 1874, 1876, 1877, and 1902 of the Act (Title 42 United States Code (U.S.C.) sections 405, 1306, 1307, 1395g, 1395h, 1395l, 1395u, 1395ii, 1395kk, 1395mm, 1395nn, and 1396a).

PURPOSE(S):

The primary purpose of the system of records is to identify if a violation(s) of a provision of the Act or a related penal or civil provision of the United States Code (U.S.C.) related to Medicare (Title XVIII), Medicaid (Title XIV), HMO/Managed Care (Title XX), and Children's Health Insurance Program (Title XXI) have been committed, determine if HHS has made a proper payment as prescribed under applicable sections of the Act and whether these programs have been abused, coordinate investigations related to Medicare, Medicaid, HMO/Managed Care, and Children's Health Insurance Program, and prevent duplications, and provide case file material to the HHS Office of the Inspector General when a case is referred for fraud investigation. Information retrieved from this system of records will also be disclosed to: support regulatory and policy functions performed within the Agency or by a contractor or consultant, support constituent requests made to a congressional representative, support litigation involving the Agency related to this system of records, and to combat fraud and abuse in certain health care programs.

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

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the FID 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, December 28, 2000, as amended by 66 FR 12434, February 26,

2001). 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 engaged by the Agency to assist in accomplishment of a CMS function relating to the purposes for this system of records and who need to have access to the records in order to assist CMS.

2. To 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.

4. 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.

5. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

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

STORAGE:

Computer diskette and on magnetic storage media.

RETRIEVABILITY:

Information can be retrieved by the name of the subject of the investigation and assigned UPIN 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 FID 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 15 years in a secure storage area with identifiers.

SYSTEM MANAGER(S) AND ADDRESSES:

Director, Program Integrity Group, Office of Financial Management, CMS, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, social security number (SSN) or UPIN, address, date of birth, and sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

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

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7).

RECORD SOURCE CATEGORIES:

Sources of information contained in this records system include data collected from FID computer files as transmitted by the contractor sites.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

HHS claims exemption of certain records (case files on active fraud investigations) in the system from notification and access procedures under 5 U.S.C. 522a (k)(2) inasmuch as these records are investigatory materials compiled for program (law) enforcement in anticipation of a criminal or administrative proceedings. (*See* Department Regulation (45 CFR 5b.11))

Appendix A. Health Insurance Claims

Medicare records are maintained at the CMS Central Office (see section 1 below for the address). Health Insurance Records of the Medicare program can also be accessed through a representative of the CMS Regional Office (see section 2 below for addresses). Medicare claims records are also maintained by private insurance organizations that share in administering provisions of the health insurance programs. These private insurance organizations, referred to as carriers and intermediaries, are under contract to the Health Care Financing Administration and the Social Security Administration to perform specific task in the Medicare program (see section three below for addresses for intermediaries, section four addresses the carriers, and section five addresses the Payment Safeguard Contractors.

I. Central Office Address

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

II. CMS Regional Offices

Boston Region—Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont. John F. Kennedy Federal Building, Room 1211, Boston, Massachusetts 02203. Office Hours: 8:30 a.m.–5 p.m.

New York Region—New Jersey, New York, Puerto Rico, Virgin Islands. 26 Federal Plaza, Room 715, New York, New York 10007, Office Hours: 8:30 a.m.–5 p.m.

Philadelphia Region—Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia. Post Office Box 8460, Philadelphia, Pennsylvania 19101. Office Hours: 8:30 a.m.–5 p.m.

Atlanta Region—Alabama, North Carolina, South Carolina, Florida, Georgia, Kentucky, Mississippi, Tennessee. 101 Marietta Street, Suite 702, Atlanta, Georgia 30223, Office Hours: 8:30 a.m.–4:30 p.m.

Chicago Region—Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin. Suite A—824, Chicago, Illinois 60604. Office Hours: 8 a.m.–4:45 p.m.

Dallas Region—Arkansas, Louisiana, New Mexico, Oklahoma, Texas, 1200 Main Tower Building, Dallas, Texas. Office Hours: 8 a.m.–4:30 p.m.

Kansas City Region—Iowa, Kansas, Missouri, Nebraska. New Federal Office Building, 601 East 12th Street Room 436, Kansas City, Missouri 64106. Office Hours: 8 a.m.–4:45 p.m.

Denver Region—Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming. Federal Office Building, 1961 Stout St Room 1185, Denver, Colorado 80294. Office Hours: 8 a.m.–4:30 p.m.

San Francisco Region—American Samoa, Arizona, California, Guam, Hawaii, Nevada. Federal Office Building, 10 Van Ness Avenue, 20th Floor, San Francisco, California 94102. Office Hours: 8 a.m.–4:30 p.m.

Seattle Region—Alaska, Idaho, Oregon, Washington. 1321 Second Avenue, Room 615, Mail Stop 211, Seattle, Washington 98101. Office Hours 8 a.m.–4:30 p.m.

III. Intermediary Addresses (Hospital Insurance)

Medicare Coordinator, Assoc. Hospital Serv. Maine (ME BC), 2 Gannett Drive South, Portland, ME 04106–6911.

Medicare Coordinator, Anthem New Hampshire, 300 Goffs Falls Road, Manchester, NH 03111–0001.

Medicare Coordinator, BC/BS Rhode Island (RI BC), 444 Westminster Street, Providence, RI 02903–3279.

Medicare Coordinator, Empire Medicare Services, 400 S. Salina Street, Syracuse, NY 13202.

Medicare Coordinator, Cooperativa, PO Box 363428, San Juan, PR 00936–3428.

Medicare Coordinator, Maryland B/C, PO Box 4368, 1946 Greenspring Ave., Timonium, MD 21093.

Medicare Coordinator, Highmark, P5103, 120 Fifth Avenue Place, Pittsburgh, PA 15222–3099.

Medicare Coordinator, United Government Services, 1515 N. Rivercenter Dr., Milwaukee, WI 53212.

Medicare Coordinator, Alabama B/C, 450 Riverchase Parkway East, Birmingham, AL 35298.

Medicare Coordinator, Florida B/C, 532 Riverside Ave., Jacksonville, FL 32202–4918.

Medicare Coordinator, Georgia B/C, PO Box 9048, 2357 Warm Springs Road, Columbus, GA 31908.

Medicare Coordinator, Mississippi B/C B MS, PO Box 23035, 3545 Lakeland Drive, Jackson, MI 39225–3035.

Medicare Coordinator, North Carolina B/C, PO Box 2291, Durham, NC 27702–2291.

Medicare Coordinator, Palmetto GBA A/RHHI, 17 Technology Circle, Columbia, SC 29203–0001.

Medicare Coordinator, Tennessee B/C, 801 Pine Street, Chattanooga, TN 37402–2555.

Medicare Coordinator, Anthem Insurance Co. (Anthm IN), PO Box 50451, 8115 Knue Road, Indianapolis, IN 46250–1936.

Medicare Coordinator, Arkansas B/C, 601 Gaines Street, Little Rock, AR 72203.

Medicare Coordinator, Group Health of Oklahoma, 1215 South Boulder, Tulsa, OK 74119–2827.

Medicare Coordinator, Trailblazer, PO Box 660156, Dallas, TX 75266–0156.

Medicare Coordinator, Cahaba GBA, Station 7, 636 Grand Avenue, Des Moines, IA 50309–2551.

Medicare Coordinator, Kansas B/C, PO Box 239, 1133 Topeka Ave., Topeka, KS 66629–0001.

Medicare Coordinator, Nebraska B/C, PO Box 3248, Main PO Station, Omaha, NE 68180–0001.

Medicare Coordinator, Mutual of Omaha, PO Box 1602, Omaha, NE 68101.

Medicare Coordinator, Montana B/C, PO Box 5017, Great Falls Div., Great Falls, MT 59403–5017.

Medicare Coordinator, Noridian, 4510 13th Avenue SW., Fargo, ND 58121–0001.

Medicare Coordinator, Utah B/C, PO Box 30270, 2455 Parleys Way, Salt Lake City, UT 84130–0270.

Medicare Coordinator, Wyoming B/C, 4000 House Avenue, Cheyenne, WY 82003.

Medicare Coordinator, Arizona B/C, PO Box 37700, Phoenix, AZ 85069.

Medicare Coordinator, UGS, PO Box 70000, Van Nuys, CA 91470–0000.

Medicare Coordinator, Regents BC, PO Box 8110 M/S D–4A, Portland, OR 97207–8110.

Medicare Coordinator, Premera BC, PO Box 2847, Seattle, WA 98111–2847.

IV. Medicare Carriers

Medicare Coordinator, NHIC, 75 Sargent William Terry Drive, Hingham, MA 02044.

Medicare Coordinator, B/S Rhode Island (RI BS), 444 Westminster Street, Providence, RI 02903–2790.

Medicare Coordinator, Trailblazer Health Enterprises, Meriden Park, 538 Preston Ave., Meriden, CT 06450.

Medicare Coordinator, Upstate Medicare Division, 11 Lewis Road, Binghamton, NY 13902.

Medicare Coordinator, Empire Medicare Services, 2651 Strang Blvd., Yorktown Heights, NY, 10598.

Medicare Coordinator, Empire Medicare Services, NJ, 300 East Park Drive, Harrisburg, PA 17106.

Medicare Coordinator, Triple S, #1441 F.D., Roosvelt Ave., Guaynabo, PR 00968.

Medicare Coordinator, Group Health Inc., 4th Floor, 88 West End Avenue, New York, NY 10023.

Medicare Coordinator, Highmark, PO Box 89065, 1800 Center Street, Camp Hill, PA 17089–9065.

Medicare Coordinator, Trailblazers Part B, 11150 McCormick Drive, Executive Plaza 3 Suite 200, Hunt Valley, MD 21031.

Medicare Coordinator, Trailblazer Health Enterprises, Virginia, PO Box 26463, Richmond, VA 23261–6463. United Medicare Coordinator, Tricenturion, 1 Tower Square, Hartford, CT 06183.

Medicare Coordinator, Alabama B/S, 450 Riverchase Parkway East, Birmingham, AL 35298.

Medicare Coordinator, Cahaba GBA, 12052 Middleground Road, Suite A, Savannah, GA 31419.

Medicare Coordinator, Florida B/S, 532 Riverside Ave, Jacksonville, FL 32202–4918.

Medicare Coordinator, Administar Federal, 9901 Linnstation Road, Louisville, KY 40223.

Medicare Coordinator, Palmetto GBA, 17 Technology Circle, Columbia, SC 29203–0001.

Medicare Coordinator, CIGNA, 2 Vantage Way, Nashville, TN 37228.

Medicare Coordinator, Railroad Retirement Board, 2743 Perimeter Parkway, Building 250, Augusta, GA 30999.

Medicare Coordinator, Cahaba GBA, Jackson Miss, PO Box 22545, Jackson, MI 39225–2545.

Medicare Coordinator, Adminastar Federal (IN), 8115 Knue Road, Indianapolis, IN 46250–1936.

Medicare Coordinator, Wisconsin Physicians Service, PO Box 8190, Madison, WI 53708–8190.

Medicare Coordinator, Nationwide Mutual Insurance Co., PO Box 16788, 1 Nationwide Plaza, Columbus, OH 43216–6788.

Medicare Coordinator, Arkansas B/S, 601 Gaines Street, Little Rock, AR 72203.

Medicare Coordinator, Arkansas-New Mexico, 601 Gaines Street, Little Rock, AR 72203.

Medicare Coordinator, Palmetto GBA–DMERC, 17 Technology Circle, Columbia, SC 29203–0001.

Medicare Coordinator, Trailblazer Health Enterprises, 901 South Central Expressway, Richardson, TX 75080.

Medicare Coordinator, Nordian, 636 Grand Avenue, Des Moines, IA 50309–2551.

Medicare Coordinator, Kansas B/S, PO Box 239, 1133 Topeka Ave., Topeka, KS 66629–0001.

Medicare Coordinator, Kansas B/S–NE, PO Box 239, 1133 Topeka Ave., Topeka, KS 66629–0239.

Medicare Coordinator, Montana B/S, PO Box 4309, Helena, MT 59601.

Medicare Coordinator, Nordian, 4305 13th Avenue South, Fargo, ND 58103–3373.

Medicare Coordinator, Noridian BCBSND (C0), 730 N. Simms #100, Golden, CO 80401–4730.

Medicare Coordinator, Noridian BCBSND (WY), 4305 13th Avenue South, Fargo, ND 58103–3373.

Medicare Coordinator, Utah B/S, PO Box 30270, 2455 Parleys Way, Salt Lake City, UT 84130–0270.

Medicare Coordinator, Transamerica Occidental, PO Box 54905, Los Angeles, CA 90054–4905.

Medicare Coordinator, NHIC—California, 450 W. East Avenue, Chico, CA 95926.

Medicare Coordinator, Cigna, Suite 254, 3150 Lakeharbor, Boise, ID 83703.

Medicare Coordinator, Cigna, Suite 506, 2 Vantage Way, Nashville, TN 37228.

V. Payment Safeguard Contractors

Medicare Coordinator, Aspen Systems Corporation, 2277 Research Blvd., Rockville, MD 20850.

Medicare Coordinator, DynCorp Electronic Data Systems (EDS, 11710 Plaza America Drive 5400 Legacy Drive, Reston, VA 20190–6017.

Medicare Coordinator, Lifecare Management Partners Mutual of Omaha Insurance Co. 6601 Little River Turnpike, Suite 300 Mutual of Omaha Plaza, Omaha, NE 68175.

Medicare Coordinator, Reliance Safeguard Solutions, Inc., PO Box 30207 400 South Salina Street, 2890 East Cottonwood Pkwy. Syracuse, NY 13202.

Medicare Coordinator, Science Applications International, Inc., 6565 Arlington Blvd., PO Box 100282, Falls Church, VA.

Medicare Coordinator, California Medical Review, Inc., Integriguard Division Federal Sector Civil Group, One Sansome Street, San Francisco, CA 94104–4448.

Medicare Coordinator, Computer Sciences Corporation, Suite 600 3120 Timanus Lane, Baltimore, MD 21244.

Medicare Coordinator, Electronic Data Systems (EDS), 11710 Plaza America Drive 5400 Legacy Drive, Plano, TX 75204.

Medicare Coordinator, TriCenturion, L.L.C., PO Box 100282, Columbia, SC 29202.

[FR Doc. 02–27337 Filed 10–25–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 02N–0445]

FDA Regulation of Combination Products; Public Hearing

AGENCY: Food and Drug Administration.

ACTION: Notice of public hearing; request for comments.

SUMMARY: The Food and Drug Administration (FDA) is announcing a public hearing to discuss the assignment, premarket review, and postmarket regulation of combination products. Combination products (defined in more detail later in this document) are products containing a combination of drugs, devices, or biological products. These products often are novel and have significant potential to enhance the public health. The purpose of the hearing is to solicit information and views from interested persons on the issues and concerns relating to the assignment, premarket review, and postmarket regulation of combination products. FDA is proposing specific questions, and the agency is interested in responses to these questions and any other pertinent information stakeholders would like to share.

DATES: The public hearing will be held on November 25, 2002, from 9 a.m. to 5 p.m. Submit written or electronic notices of participation by close of business on November 8, 2002. Written and electronic comments will be accepted until January 24, 2003.

ADDRESSES: The public hearing will be held at the DoubleTree Hotel, 1750 Rockville Pike, Rockville, MD. Directions to the hotel can be found at *http://www.doubletreerockville.com*.

Submit written or electronic notices of participation and comments to the Dockets Management Branch (HFA–305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852; or e-mail FDADockets@oc.fda.gov; or on the Internet at *http://www.accessdata.fda.gov/scripts/oc/dockets/commentdocket.cfm*. Transcripts of the hearing will be available for review at the Dockets Management Branch (see address in previous sentence) and on the Internet at *http://www.fda.gov/ohrms/dockets*.

FOR FURTHER INFORMATION CONTACT: Mark D. Kramer, Combination Products Program (HF–7), Food and Drug Administration, 5600 Fishers Lane, rm. 14B–03, Rockville, MD 20857, 301–827–3390, FAX 301–480–8039, e-mail: *mkramer@oc.fda.gov*.

Registration Information and Requests for Oral Presentation

Preregistration by written notice is necessary to ensure participation. The procedures governing the hearing are found in part 15 (21 CFR part 15). To register to attend the hearing, submit your name, title, business affiliation, address, telephone, fax number, and e-mail address. If you wish to make an oral presentation during the open public comment period of the hearing, you must state your intention on your registration form or with the registration contact person listed (*see* **FOR FURTHER INFORMATION CONTACT**). You must submit a written statement at the time of registration for each discussion question you wish to address, the names and addresses of all individuals that plan to participate, and the approximate time requested to make your presentation. Electronic registration for this hearing is available at *http://www.accessdata.fda.gov/scripts/oc/dockets/meetings/meetingdocket.cfm*. Registrations will be accepted on a first-come, first-served basis. Individuals who register to make an oral presentation will be notified of the scheduled time for their presentation prior to the hearing. Depending on the number of presentations, FDA may need to limit the time allotted for each presentation. All participants are encouraged to attend the entire day. Presenters must submit two copies of each presentation given. If you need special accommodations due to a disability, please inform the registration contact person when you register. Presentations will be limited to the questions and subject matter identified in section III of this document.

SUPPLEMENTARY INFORMATION:

I. Background

The Safe Medical Devices Act (SMDA) of 1990 explicitly recognized the existence of products that ''constitute a combination of a drug, device, or biological product'' and provided a mechanism for determining which agency component would be assigned the administrative responsibility of regulating a particular combination product (21 U.S.C. 353(g)). The Food and Drug Administration Modernization Act of 1997 (FDAMA) further refined the assignment process by providing a mechanism to request that FDA classify a product as a drug, biological product, device, or a combination product, in addition to determining which agency component will be assigned to regulate the product (21 U.S.C. 360bbb–2).

As defined in § 3.2(e) (21 CFR 3.2(e)), the term combination product means a product comprised of two or more different regulated components, e.g., drug, device, or biologic (for example, a syringe prefilled with a drug); or two or more separate products packaged together as one unit (for example, a kit containing drapes, needles, a syringe, a local anesthetic and a topical antiseptic). A combination product is also defined to include a product that is intended for use only with an approved product where both are required to achieve the intended use, indication, or effect, and the labeling of the approved product needs to be changed to reflect this use. For example, if a device to aerosolize medication works only with a specific aerosolized drug, the device would be labeled for use with this drug and the two products would be a combination product. Finally, the combination product definition