collection of information, including any of the following subjects: (1) The necessity and utility of the proposed information collection for the proper performance of the agency's functions; (2) the accuracy of the estimated burden; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) the use of automated collection techniques or other forms of information technology to minimize the information collection burden.

Type of Information Collection Request: Extension of a currently approved collection; *Title of Information Collection:* Informatics, Telemedicine, and Education Demonstration Project; *Form No.:* CMS–10014 (OMB# 0938–0806); *Use:* Section 4207 of the Balanced Budget Act of 1997 mandated CMS to conduct a demonstration project to evaluate the effectiveness of advanced computer and telecommunications technology (''telemedicine'') to manage the care of people with diabetes. CMS issued a request for proposals and, after review of the responses, selected a consortium led by Columbia University to conduct this project; *Frequency:* Semi-annually; *Affected Public:* Business or other for profit, individuals or households; *Number of Respondents:* 5,550; *Total Annual Responses:* 10,043; *Total Annual Hours:* 19,999.

To obtain copies of the supporting statement and any related forms for the proposed paperwork collections referenced above, access CMS Web Site address at http://www.hcfa.gov/regs/prdact95.htm, or E-mail your request, including your address, phone number, OMB number, and CMS document identifier, *to Paperwork@hcfa.gov*, or call the Reports Clearance Office on (410) 786–1326. Written comments and recommendations for the proposed information collections must be mailed within 30 days of this notice directly to the OMB desk officer: OMB Human Resources and Housing Branch, Attention: New Executive Office Building, Room 10235, Washington, DC 20503.

Dated: May 15, 2002.

John P. Burke III,

Paperwork Reduction Act Team Leader, CMS Reports Clearance Officer, CMS Office of Information Services, Security and Standards Group, Division of CMS Enterprise Standards.

[FR Doc. 02–13184 Filed 5–24–02; 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) (formerly the Health Care Financing Administration).

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 ''Non-Medicare Beneficiary Workers'' Compensation (WC) Set-aside File (WCSAF),'' HHS/CMS/CMM No. 09–70–0537. The primary purpose of the non-Medicare beneficiary WCSAF is to maintain a file of individuals who were injured while employed, are not currently Medicare beneficiaries, and received a WC Set-aside Arrangement, as part of a WC settlement, that is intended to pay for future medical expenses in place of future Medicare benefits. The 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; to another Federal or State agency to contribute to the accuracy of CMS' proper payment of Medicare benefits, to enable such agency to administer a Federal health benefits program, or to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; support constituent requests made to a Congressional representative; support litigation involving the agency; and support research, evaluation, and for payment related projects; and to disclose individual-specific information for the purpose of combating fraud and abuse in health benefits programs administered by CMS.

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 May 8, 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: Donna Kettish, Division of Benefit Coordination, Benefits Operations Group, Center for Medicare Management, CMS, S1–05–06, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is (410) 786–5462.

SUPPLEMENTARY INFORMATION:

I. Description of the New System of Records

A. Statutory and Regulatory Basis for System of Records

Section 1862 (b) (2) of the Social Security Act (the Act), requires that Medicare payment may not be made for any item or service to the extent that payment has been made under a WC law or plan. This section of the Act and 42 CFR 411.46 require CMS to exclude payments once the injured individual becomes a Medicare beneficiary when payment should be made from WC funds which are always primary to Medicare payment.

B. Background

CMS is responsible for safeguarding the fiscal integrity of the Medicare Program. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the ''Medicare Integrity Program,'' enabling CMS to competitively award contracts with entities to promote the integrity of the Medicare Program. The Coordination of Benefit Contractor (COBC) is one of those specialized contractors hired to increase efficiency and effectiveness by ensuring that benefit payments are made by the appropriate payer by coordinating Medicare and other benefit payments.

The Electronic Correspondence Referral System (ECRS) is currently used to transfer data between CMS's Medicare contractors and the COBC to establish Medicare Secondary Payer periods of coverage on CMS's Common Working File (CWF). The CWF is a CMS system, containing Medicare beneficiary eligibility information, that is used for verification and validation purposes to ensure Medicare claims are paid properly and by the appropriate payer. ECRS is being enhanced to transfer WC Set-aside Arrangement data from CMS Regional Offices (RO) to the COBC for Medicare beneficiaries and non-Medicare beneficiaries who have an approved WC Set-aside Arrangement to cover future medical costs resulting from an injury incurred while employed. If the injury results in disability payments from the Social Security Administration (SSA), there is a reasonable expectation that the injured individual will also be eligible for Medicare benefits some time after the WC settlement is made.

The ROs will transfer the WC Set-aside Arrangement information via ECRS for non-Medicare beneficiaries once they approve the arrangement. The COBC will maintain ECRS transferred data in the WCSAF for future matching purposes. The COBC will ''match'' non-beneficiary WCSAF data against the file it receives each month of new Medicare eligibles to identify any non-beneficiaries with impending Medicare entitlement. Once a match occurs, the existence of a WC Set-aside Arrangement will be reflected on the new beneficiary's CWF record and a Lead Medicare Contractor will be assigned for coordination of the expenditures from the WC Set-aside Arrangement.

CMS is drawn into a civil action resulting from a WC claim in a consulting position to ensure that a legal settlement involving an injured worker considers Medicare's interest with respect to future claims. CMS RO approval of a Medicare Set-aside Arrangement helps direct the treatment of future disorders or health claims by the injured worker, ensuring he/she is adequately covered for long-term care resulting from their WC injury, first by the Medicare Set-aside Arrangement and then by Medicare if necessary.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The WCSAF includes standard data for identification including the name, address, date of birth, Social Security Number, date of the WC injury/incident, injury diagnosis code(s), effective date and amount of the WC Set-aside Arrangement. In addition, data will be included to enable CMS to manage the WC Set-aside Arrangement information when it becomes part of the beneficiary's record on the CWF. These data include the WC carrier, the administrator of the Set-aside Arrangement, and the attorney that prepared the arrangement.

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

CMS will only disclose the minimum personal data necessary to achieve the purpose of the WCSAF. 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., ensuring that benefit payments are made by the appropriate payer by coordinating Medicare and other benefit payments.

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 WCSAF 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 the agency of a State government, or established by State law,

for purposes of ensuring that benefit payments are made by the appropriate payer by coordinating Medicare and other benefit payments.

WCSAF data may be released to the State only on those injured individuals who are not currently Medicare beneficiaries but receive a WC Set-aside Arrangement that is intended to pay for future medical expenses in place of future Medicare benefits.

3. To another Federal or State agency:

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

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

Other Federal or State agencies in their administration of a Federal health program may require WCSAF information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper payment for services provided. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purpose for which CMS collects the information.

4. To an individual or organization for research, evaluation or epidemiological projects related to the prevention of disease or disability, the restoration or maintenance of health, or for understanding and improving payment projects.

The WCSAF data will provide the research and evaluations a broader, longitudinal, national perspective of the status of injured individuals that are not currently Medicare beneficiaries but receive a WC Set-aside Arrangement that is intended to pay for future medical expenses in place of future Medicare benefits

5. 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.

6. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. Any employee of the agency in his or her official capacity; or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. The United States Government; is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation.

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court or adjudicatory body involved. 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.

7. To a CMS contractor (including, but not necessarily limited to 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.

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 CMS functions relating to the purpose of combating fraud and abuse.

CMS occasionally contracts out certain of its functions when this 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 (like ensuring 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 those stated in II.B, above), 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 to return or destroy all information.

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

Other State agencies in their administration of a Federal health program may require WCSAF information for the purpose of preventing, deterring, discovering, detecting, investigating, examining, prosecuting, suing with respect to, defending against, correcting, remedying, or otherwise combating such fraud and abuse in such programs. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purpose for which CMS collects the information.

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 WCSAF 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 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 WCSAF data. WCSAF 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 WCSAF 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 9, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0537

SYSTEM NAME:

Non-Medicare Beneficiary Workers' Compensation (WC) Set-aside File, (WCSAF).

SECURITY CLASSIFICATION:

Level 3, Privacy Act Sensitive.

SYSTEM LOCATION:

Group Health Incorporated, 25 Broadway, NY, NY 10004.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system of records will contain data on non-Medicare beneficiaries that receive a WC Set-aside Arrangement, as part of a WC settlement, that is intended to pay for future medical expenses in place of future Medicare benefits.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system of records will contain the individual-level identifying data including such as the name, address, date of birth, Social Security Number (SSN), date of the WC injury/incident, injury diagnosis code(s), effective date and amount of the WC Set-aside Arrangement. In addition, data will be included to enable CMS to manage the WC Set-aside Arrangement information when it becomes part of a beneficiary's record on the Common Working File (CWF). These data include the WC carrier, the administrator of the WC Set-aside Arrangement, and the attorney that prepared the arrangement.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Sec. 1862(b)(2) of the Social Security Act (the Act) and 42 CFR 411.46.

PURPOSE(S):

The primary purpose of the non-Medicare beneficiary WCSAF is to maintain a file about individuals who were injured while employed, are not currently Medicare beneficiaries, and received a WC Set-aside Arrangement, as part of a WC settlement, that is intended to pay for future medical expenses in place of future Medicare benefits. The 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; to another Federal or State agency to contribute to the accuracy of CMS' proper payment of Medicare benefits, to enable such agency to administer a Federal health benefits program, or to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; support constituent requests made to a Congressional representative; support litigation involving the agency; and support research, evaluation, and for payment related projects; and to disclose individual-specific information for the purpose of combating fraud and abuse in health benefits programs administered by CMS.

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 WCSAF 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 the agency of a State government, or established by State law, for purposes of ensuring that benefit payments are made by the appropriate payer by coordinating Medicare and other benefit payments.

3. To another Federal or State agency:

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

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

4. To an individual or organization for research, evaluation or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, or for understanding and improving payment projects.

5. 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.

6. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof; or

b. Any employee of the agency in his or her official capacity; or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee; or

d. The United States Government;

is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

7. To a CMS contractor (including, but not necessarily limited to 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.

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

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

STORAGE:

All records are stored on magnetic media.

RETRIEVABILITY:

The Social Security 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:

CMS will retain identifiable WCSAF data for a period of 6 years and 3 months unless the injured individual becomes a Medicare beneficiary prior to that period of time. When either of these criteria is met, the information stored on the injured individual will be deleted from the WCSAF.

SYSTEM MANAGER(S) AND ADDRESS:

CMS, Center for Medicare Management, Benefits Operations Group, Director, Division of Benefit Coordination, 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, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), address, date of birth, date of WC injury/incident, diagnosis, effective date and amount of the WC Set-aside Arrangement. (Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay).

RECORD ACCESS PROCEDURE:

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

CONTESTING RECORD PROCEDURES:

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

RECORD SOURCE CATEGORIES:

The Electronic Correspondence Referral System (ECRS), Medicare contractors and the Coordination of Benefit Contractor (COBC), Common Working File, CMS Regional Offices (RO), Medicare beneficiaries and non-Medicare beneficiaries that have an approved WC Set-aside Arrangement to cover future medical costs resulting from an injury incurred while employed and the Social Security Administration (SSA).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–13190 Filed 5–24–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 99E–1086]

Determination of Regulatory Review Period for Purposes of Patent Extension; ENBREL

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA) has determined the regulatory review period for ENBREL and is publishing this notice of that determination as required by law. FDA has made the determination because of the submission of an application to the Director of Patents and Trademarks, Department of Commerce, for the extension of a patent which claims that human biological product.

ADDRESSES: Submit written comments and petitions to the Dockets Management Branch (HFA–305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852.

FOR FURTHER INFORMATION CONTACT: Claudia Grillo, Office of Regulatory Policy (HFD–007), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301–827–4565.

SUPPLEMENTARY INFORMATION: The Drug Price Competition and Patent Term Restoration Act of 1984 (Public Law 98–417) and the Generic Animal Drug and Patent Term Restoration Act (Public Law 100–670) generally provide that a patent may be extended for a period of up to 5 years so long as the patented item (human drug product, animal drug product, medical device, food additive, or color additive) was subject to regulatory review by FDA before the item was marketed. Under these acts, a product's regulatory review period forms the basis for determining the amount of extension an applicant may receive.

A regulatory review period consists of two periods of time: A testing phase and an approval phase. For human biological products, the testing phase begins when the exemption to permit the clinical investigations of the biological becomes effective and runs until the approval phase begins. The approval phase starts with the initial submission of an application to market the human biological product and continues until FDA grants permission to market the biological product. Although only a portion of a regulatory review period may count toward the actual amount of extension that the Commissioner of Patents and Trademarks may award (for example, half the testing phase must be subtracted as well as any time that may have occurred before the patent was issued), FDA's determination of the length of a regulatory review period for a human biological product will include all of the testing phase and approval phase as specified in 35 U.S.C. 156(g)(1)(B).

FDA recently approved for marketing the human biological product ENBREL (etanercept). ENBREL is indicated for the reduction in signs and symptoms of moderately to severely active rheumatoid arthritis in patients who have had an inadequate response to one or more disease-modifying antirheumatic drugs. Subsequent to this approval, the Patent and Trademark Office received a patent term restoration application for ENBREL (U.S. Patent No. 5,712,155) from Immunex Corp., and the Patent and Trademark Office requested FDA's assistance in determining this patent's eligibility for patent term restoration. In a letter dated August 7, 2000, FDA advised the Patent and Trademark Office that this human biological product had undergone a regulatory review period and that the approval of ENBREL represented the first permitted commercial marketing or use of the product. Shortly thereafter, the Patent and Trademark Office