manager who will require the system name, identification number, address, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

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

CONTESTING RECORD PROCEDURES:

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

RECORD SOURCE CATEGORIES:

Sources of information contained in this records system include data collected from the application which the supplier completes to obtain Medicare billing numbers. (CMS Form 192-prior to August 1996, CMS Form 885, April 1996–May 1997, and CMS Form 855S-after May, 1997).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–18168 Filed 7–22–02; 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 Modified or Altered System

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (formerly the Health Care Financing Administration).

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 an SOR, ''Intern and Resident Information System (IRIS), No. 09–70–0524.'' We will broaden the scope of this system to include information on interns and residents (IRs) required in Title 42 Code of Federal Regulations (CFR) § 412.105 (Special treatment: Hospitals that incur indirect costs for graduate medical education programs) and 42 CFR 413.86 (Direct graduate medical education payments). We are also deleting published routine use number 3 authorizing disclosures to contractors, number 6 authorizing disclosures to researchers, and an unnumbered routine use which authorizes the release of information to the Social Security Administration (SSA).

Proposed routine use number 1 will now cover disclosures previously allowed by routine use number 3 pertaining to contractors. Access to the data from this system to SSA will be accomplished by adding a new routine use number 4, which authorizes release of information in this system to ''another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent.'' Routine use number 6 authorizing release to researchers is being deleted because the very specific nature of the data collected is not sought for research purposes.

The security classification previously reported as ''None'' will be modified to reflect that the data in this system are considered to be ''Level Three Privacy Act Sensitive.'' We are modifying the language in the remaining routine uses to provide clarity to CMS's intention to disclose individual-specific information contained in this system. 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 SORs.

The primary purpose of the SOR is to ensure that no IRs are counted by the Medicare program as more than one full-time equivalent (FTE) employee in the calculation of payments for the costs of direct graduate medical education (GME) and indirect medical education (IME). Information retrieved from this SOR will also be disclosed to: support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant, providers and suppliers of services, third-party contacts where necessary to establish or verify information, another Federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, support constituent requests made to a congressional representative, support litigation involving the Agency, and combat fraud and abuse in certain health benefits programs. We have provided background information about the modified system in the ''Supplementary Information'' section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

EFFECTIVE DATES: CMS filed a modified or altered 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 June 24, 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 (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 am.–3 pm., Eastern daylight time.

FOR FURTHER INFORMATION CONTACT: Milton Jacobson, Division of Financial Integrity, Office of Financial Management, CMS, Room C3–14–00, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–7553.

SUPPLEMENTARY INFORMATION:

I. Description of the Modified System

A. Statutory and Regulatory Basis for the SOR

In 1990, CMS established a SOR under the authority of sections 1886(d)(5)(B) and 1886(h) of the Social Security Act (the Act) (42 U.S.C. 1395ww(d)(5)(B) and 1395ww(h)). Notice of this system, ''Intern and Resident Information System,'' System No. 09–70–0524, was published in the **Federal Register** (FR) at 55 FR 51163–51165 (Dec. 12, 1990). 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 was revised and a third deleted. This system was established to ensure that no IRs are counted by the Medicare program as more than one FTE employee in the calculation of payments for the costs of direct GME and IME. The system contains information on IRs in accordance with 42 CFR 413.86(I) for GME and 42 CFR 412.105(f)(2) for IME. This information includes names and social security numbers of IRs who worked at the hospital in approved GME programs during the hospital's cost reporting period. It also discloses information on each IRs medical specialty (e.g., type of residency program), and the number of years each IRs has completed in all types of residency programs. Hospitals are required to submit the information on IRIS diskettes along with their cost reports to their fiscal intermediaries (FI) in accordance with 42 CFR 413.24(f)(5)(I).

The FIs are the primary user of information from IRIS diskettes. They use the information to detect duplicates of IRs being over reported by two or more of their serviced hospitals. FIs with confirmed duplicates of over reported IR at their serviced hospitals can make adjustments to FTE counts of these IRs on cost report settlements.

The FI also use IRIS diskettes for transmitting data on consolidated diskettes to CMS. CMS uploads the data into its mainframe computer for data storage and retrieval purposes. The computer is used to create duplicate reports of over reported IRs for the FI and CMS.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The system includes the following information for each IR: name, social security number; name of medical, osteopathic, or podiatric school graduated from and date of graduation, type of dental degree and date of graduation, type of residency program for the medical specialty, number of years completed in all types of residency programs, foreign medical school graduation date and certification date, name of employer (e.g., hospital, university, corporation) paying the salary, the percentage of time spent working in either the inpatient areas of the hospital subject to the Prospective Payment System or in the outpatient areas of the hospital or in a non-hospital setting under agreement with the hospital for IME, the percentage of time spent working in any area of the hospital complex or in a non-provider setting under agreement with the hospital for GME, the start and end dates assigned to the hospital and any hospital-based providers (assignment periods) during the hospital's cost reporting period, the start and end dates assigned to any non-hospital or non-provider setting in connection with approved residency programs (assignment periods) during the hospital's cost reporting period, and the full-time or part-time percentage during each assignment period.

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 IRIS information that can be associated with an individual as provided for under ''Section III. Proposed Routine Use Disclosures of Data in the System.'' Both identifiable and non-identifiable data may be disclosed under a routine use.

We will only disclose the minimum personal data necessary to achieve the purpose of IRIS. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure and only after CMS:

1. Determines that the use or disclosure is consistent with the reason data is being collected; e.g., that no IRs are counted by the Medicare program as more than one full-time equivalent (FTE) employee in the calculation of payments for the costs of direct graduate medical education (GME) and indirect medical education (IME).

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

a. 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

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

3. Requires the information recipient to:

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

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

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

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosures Under Routine Use

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

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

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

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

2. To providers and suppliers of services (and their authorized billing agents) directly or dealing through fiscal intermediaries or carriers, for

administration of provisions of Title XVIII of the Social Security Act.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual agreement with providers and suppliers of services to assist in accomplishing CMS functions relating to purposes for this SOR.

3. To third-party contacts where necessary to establish or verify information provided on or by IRs.

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 CMS functions relating to purposes for this system of records.

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

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 IRIS information in order to support evaluations and monitoring of reimbursement for services provided.

SSA may require IRIS data to enable it to assist in the implementation and maintenance of the Medicare program.

State licensing boards may require IRIS data to enable them to assist in the review of activities related to IRs in their state.

The Medicare Payment Advisory Commission and Congressional Budget Office may require IRIS data to assist in certain budgetary and planning activities related to IR status.

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 may request the help of a Member of Congress in resolving an issue relating to a matter before CMS. The Member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

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

a. The agency or any component thereof, or

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

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

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

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

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

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

Other agencies may require IRIS information for the purpose of combating fraud and abuse in such Federally funded programs.

B. Additional Circumstances Affecting Routine Use Disclosures

This SOR contains Protected Health Information as defined by HHS regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 (12–28–00), as amended by 66 FR 12434 (2–26–01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information''.

In addition, our policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

IV. Safeguards

A. Administrative Safeguards

The IRIS 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 the Office and Management and Budget Circular A–130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems.'' Paragraphs A-C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

Authorized users: Personnel having access to the system have been trained in Privacy Act and systems security requirements. Employees and contractors who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural,

and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. In addition, CMS is monitoring the authorized users to ensure against excessive or unauthorized use. Records are used in a designated work area or workstation and the system location is attended at all times during working hours.

To 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 patient identification information; and
- *Submitter* class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards

All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the IRIS 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 which grant 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 Services (RAS)—Windows NT RAS security handles resource access control. Access to NT resources is controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

There are several levels of security found in the IRIS system. Windows NT provides much of the overall system security. The Windows NT security model is designed to meet the C2-level criteria as defined by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria document (DoD 5200.28–STD, December 1985). Netscape Enterprise Server is the security mechanism for all transmission connections to the system. As a result, Netscape controls all information access requests. Anti-virus software is applied at both the workstation and NT server levels.

Access to different areas on the Windows NT server are maintained through the use of file, directory and share level permissions. These different levels of access control provide security that is managed at the user and group level within the NT domain. The file and directory level access controls rely on the presence of an NT File System hard drive partition. This provides the most robust security and is tied directly to the file system. Windows NT security is applied at both the workstation and NT server levels.

C. Procedural Safeguards

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

V. Effect of the Modified SOR 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 IRIS data. IRIS 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 IRIS 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: June 24, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

System No. 09–70–0524

SYSTEM NAME:

''Intern and Resident Information System (IRIS),'' HHS/CMS/OFM.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive.

SYSTEM LOCATION:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Interns and residents (IRs) in programs approved under 42 CFR

413.85, working in all areas of the hospital complex, or other freestanding providers, as well as non-hospital or non-provider settings on or after July 1, 1985.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes the following information for each IR: name, social security number, name of medical, osteopathic, or podiatric school graduated from and date of graduation, type of dental degree and date of graduation, type of residency program for the medical specialty, number of years completed in all types of residency programs, foreign medical school graduation date and certification date, name of employer (e.g., hospital, university, corporation) paying the salary, the percentage of time spent working in either the inpatient areas of the hospital subject to PPS or in the outpatient areas of the hospital or in a non-hospital setting under agreement with the hospital for IME, the percentage of time spent working in any area of the hospital complex or in a non-provider setting under agreement with the hospital for GME, the start and end dates assigned to the hospital and any hospital-based providers (assignment periods) during the hospital's cost reporting period, the start and end dates assigned to any non-hospital or non-provider setting in connection with approved residency programs (assignment periods) during the hospital's cost reporting period, and the full-time or part-time percentage during each assignment period.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under the provisions of §§ 1886(d)(5)(B) and 1886 (h) of (the Act) (42 U.S.C. 195ww(d)(5)(B) and 1395ww (h).

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the system of records is to ensure that no IRs is counted by the Medicare program as more than one FTE employee in the calculation of payments for the costs of direct GME and IME. Information retrieved from this system of records will also be disclosed to: providers and suppliers of services, third-party contacts where necessary to establish or verify information, support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant, another Federal or state agency 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 combat fraud and abuse in certain health benefits programs.

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

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the IRIS 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 have provided a brief explanation of the routine uses we are proposing to establish or modify for 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 providers and suppliers of services (and their authorized billing agents) directly or dealing through fiscal intermediaries or carriers, for administration of provisions of Title XVIII.

3. To third-party contacts where necessary to establish or verify information provided on or by IRs.

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

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

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.

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.

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

Computer diskette and on magnetic storage media.

RETRIEVABILITY

Information can be retrieved by name and social security number of the IR.

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 IRIS. 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. Systems securities are established in accordance with the Department of Health and Human Services (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 in a secure storage area with identifiers. Disposal occurs three years from the last action on the hospital's cost report, and should be coordinated with disposal of the reports.

SYSTEM MANAGER AND ADDRESS:

Director, Division of Financial Integrity, Office of Financial Management, CMS, 7500 Security Boulevard, C3–14–00, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the systems manager who will require the system name, SSN, address, date of birth, 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:

Data for this system is collected from IRIS diskettes as transmitted by the hospitals.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–18169 Filed 7–22–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 02N–0055]

Agency Information Collection Activities; Announcement of OMB Approval; Infant Formula Recall Regulations

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA) is announcing that a collection of information entitled ''Infant Formula Recall Regulations'' has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995.

FOR FURTHER INFORMATION CONTACT: Peggy Schlosburg, Office of Information Resources Management (HFA–250), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301–827–1223.

SUPPLEMENTARY INFORMATION: In the **Federal Register** of June 6, 2002 (67 FR 39011), the agency announced that the proposed information collection had been submitted to OMB for review and clearance under 44 U.S.C. 3507. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has now approved the information collection and has assigned OMB control number 0910–0188. The approval expires on July 31, 2005. A copy of the supporting statement for this information collection is available on the Internet at http://www.fda.gov/ohrms/dockets.

Dated: July 17, 2002.

Margaret M. Dotzel,

Associate Commissioner for Policy.

[FR Doc. 02–18557 Filed 7–22–02; 8:45 am]

BILLING CODE 4160–01–S

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Government-Owned Inventions; Availability for Licensing

AGENCY: National Institutes of Health, Public Health Service, DHHS.

ACTION: Notice.

SUMMARY: The inventions listed below are owned by agencies of the U.S. Government and are available for licensing in the U.S. in accordance with 35 U.S.C. 207 to achieve expeditious commercialization of results of federally-funded research and development. Foreign patent applications are filed on selected inventions to extend market coverage for companies and may also be available for licensing.

ADDRESSES: Licensing information and copies of the U.S. patent applications listed below may be obtained by writing to the indicated licensing contact at the Office of Technology Transfer, National Institutes of Health, 6011 Executive Boulevard, Suite 325, Rockville, Maryland 20852–3804; telephone: 301/496–7057; fax: 301/402–0220. A signed Confidential Disclosure Agreement will be required to receive copies of the patent applications.

Methods for Treating Cancer in Humans Using IL–21

Patrick Hwu, M.D. and Gang Wang, Ph.D. (NCI)

U.S. Patent Application No. 60/368,438 filed on March 27, 2002

Licensing Contact: Jonathan Dixon; 301/496–7056 ext. 270; e-mail: *dixonj@od.nih.gov*

The present invention discloses the use of IL–21 for cancer therapy and/or cancer prevention. When compared to similar cytokines, IL–21 has shown substantial anticancer activity and reduced toxicity in murine models.

IL–21 belongs to the class I family of cytokines and is closely related to IL–2 and IL–15. Some cancer patients have shown significant response to administration of IL–2. However, IL–2 has also been associated with severe toxicity leading to a variety of undesirable side effects. This invention attempts to resolve the toxicity concerns and presents a new therapy for cancer prevention and treatment.

Amine Modified Random Primers for Microarray Detection

Charles Xiang and Michael J. Brownstein (NIMH)

DHHS Reference No. E–098–01/1 filed 11 Apr 2002