researchers' data security procedures will protect confidentiality.

Records may be disclosed by CDC in connection with public health activities to the Social Security Administration for sources of locating information to accomplish the research or program purposes for which the records were collected.

Records subject to the Privacy Act are disclosed to private firms for data entry, computer systems analysis and computer programming services. The contractors promptly return data entry records after the contracted work is completed. The contractors are required to maintain Privacy Act safeguards.

Records may be disclosed to appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

IV. Effects of the Proposed System of Records on Individual Rights

The routine uses proposed for this System are compatible with the stated purpose of the System:

The first routine use permits an individual may learn if a record exists about himself or herself by contacting the system manager at the address above. Requesters in person must provide driver's license or other positive identification. Individuals who do not appear in person must either: (1) Submit a notarized request to verify their identity; or (2) certify that they are the individuals they claim to be and that they understand that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act subject to a $5,000 fine.

An individual who requests notification of or access to medical records shall, at the time the request is made, designate in writing a responsible representative who is willing to review the record and inform the subject individual of its contents at the representative's discretion.

The following information must be provided when requesting notification: (1) Full name; (2) the approximate date and place of the study, if known; and (3) nature of the questionnaire or study in which the requester participated.

Same as notification procedures. Requesters should also reasonably specify the record contents being sought. An accounting of disclosures that have been made of the record, if any, may be requested.

V. Safeguards

The records in this System are stored in file folders. Service fellow personnel data is also maintained in an automated database. The records in this System are retrieved by the name of the individual, fellow, or guest researcher.

The records in this System have the following safeguards in place to maintain and protect the information as it relates to Authorized users, physical and procedural safeguards:

Authorized users—Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control and Prevention (CDC), as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

Physical Safeguards—Locked cabinets in locked rooms, electronic anti-intrusion devices in operation at the Federal Records Center, security guard service in buildings, personnel screening of visitors.

Procedural Safeguards—Users of individually identified data protect information from public scrutiny, and only specifically authorized personnel may be admitted to the record storage area. CDC employees who maintain records are instructed to check with the system manager prior to making disclosures of data.

Implementation Guidelines: The safeguards outlined above in accordance with the Chapter 45–13, "Safeguarding Records Contained in Systems of Records," of the HHS General Administration Manual.

The records in this System are retained and disposed of in the following way: Records are maintained in agency for three years. Personal identifiers are destroyed as soon as the system has stabilized, and statistical summaries can be run. Disposal methods include burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records destroyed by paper recycling process when 20 years old, unless needed for further study.

VI. OMB Control Numbers, Expiration Dates, and Titles of Information Collection

A. *Full Title:* "Study at Work Sites Where Agents Suspected of Being Occupational Hazards Exist, HHS/CDC/NIOSH."

OMB Control Number: 09–20–0118.

Expiration Date: TBD.

VII. Supporting Documentation

A. Preamble and Proposed Notice of System for publication in the **Federal Register**.

B. *Agency Rules:* None.

C. *Exemption Requested:* None.

D. *Computer Matching Report:* The new system does not require a matching report in accordance with the computer matching provisions of the Privacy Act.

[FR Doc. 2010–33016 Filed 1–24–11; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Privacy Act of 1974; Report of Modified or Altered System of Records

AGENCY: National Center for Infectious Diseases (NCID), Department of Health and Human Services (DHHS).

ACTION: Notification of Proposed Altered System of Records.

SUMMARY: The Department of Health and Human Services proposes to alter System of Records, 09–20–0136, "Epidemiologic Studies and Surveillance of Disease Problems, HHS/CDC/NCID." HHS is proposing to add the following Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) Memoranda (M) 07–16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information:

To appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

These records will be maintained by the National Center for Infectious Diseases (NCID).

DATES: Comments must be received on or before February 24, 2011. The proposed altered System of Records will be effective 40 days from the date submitted to the OMB, unless NCID receives comments that would result in a contrary determination.

ADDRESSES: You may submit comments, identified by the Privacy Act System of Record Number 09–20–0136:

- *Federal eRulemaking Portal: http://regulations.gov*. Follow the instructions for submitting comments.
- *E-mail:* Include PA SOR number 09–20–0136 in the subject line of the message.

• *Phone:* 770/488–8660 (not a toll-free number).
• *Fax:* 770/488–8659.
• *Mail:* HHS/CDC Senior Official for Privacy (SOP), Office of the Chief Information Security Officer (OCISO), 4770 Buford Highway—M/S: F–35, Chamblee, GA 30341.
• *Hand Delivery/Courier:* HHS/CDC Senior Official for Privacy (SOP), Office of the Chief Information Security Officer (OCISO), 4770 Buford Highway—M/S: F–35, Chamblee, GA 30341.
• Comments received will be available for inspection and copying at this same address from 9 a.m. to 3 p.m., Monday through Friday, Federal holidays excepted.

SUPPLEMENTARY INFORMATION: NCID proposes to alter System of Records, No. 09–20–0136, "Epidemiologic Studies and Surveillance of Disease Problems, HHS/CDC/NCID." This record system enables Centers for Disease Control and Prevention (CDC) officials to better understand disease patterns in the United States, develop programs for prevention and control of health problems, and communicate new knowledge to the health community.

This System of Record Notice is being altered to add the Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) memorandum dated May 22, 2007.

The following notice is written in the present tense, rather than the future tense, in order to avoid the unnecessary expenditure of public funds to republish the notice after the System has become effective.

Dated: December 11, 2009.

James D. Seligman,

Chief Information Officer, Centers for Disease Control and Prevention.

Editorial Note: This document was received at the Office of the Federal Register on December 27, 2010.

Department of Health and Human Services (HHS)

Centers for Disease Control and Prevention (CDC)

National Center for Infectious Diseases (NCID)

Epidemiologic Studies and Surveillance of Disease Problems—Report of Modified or Altered System of Records

Narrative Statement

I. Background and Purpose of the System

A. Background

The Department of Health and Human Services proposes to alter System of Records, No. 09–20–0136 "Epidemiologic Studies and Surveillance of Disease Problems, HHS/CDC/NCID." HHS is proposing to add the following Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) Memoranda (M) 07–16, Safeguarding Against and responding to the Breach of Personally Identifiable Information:

To appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

B. Purpose

This record system enables Centers for Disease Control and Prevention (CDC) officials to better understand disease patterns in the United States, develop programs for prevention and control of health problems, and communicate new knowledge to the health community.

II. Authority for Maintenance of the System

Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241); and Sections 304, 306 and 308(d) which discuss authority and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242b, 242k, and 242m(d)).

III. Proposed Routine Use Disclosures of Data in the System

The following routine uses apply to all records in this system except those maintained under an assurance of confidentiality provided by Section 308(d) of the Public Health Service Act (unless expressly authorized in the consent form or stipulated in the Assurance Statement):

A record may be disclosed for a research purpose, when the Department:

(A) Has determined that the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained;

(B) has determined that the research purpose (1) cannot be reasonably accomplished unless the record is provided in individually identifiable form, and (2) warrants the risk to the privacy of the individual that additional exposure of the record might bring;

(C) has required the recipient to (1) establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, (2) remove or destroy the information that identifies the individual at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project, unless the recipient has presented adequate justification of a research or health nature for retaining such information, and (3) make no further use or disclosure of the record except (a) in emergency circumstances affecting the health or safety of any individual, (b) for use in another research project, under these same conditions, and with written authorization of the Department, (c) for disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the purpose of the audit, or (d) when required by law;

(D) Has secured a written statement attesting to the recipient's understanding of, and willingness to abide by these provisions.

Disclosure may be made to organizations deemed qualified by the Secretary to carry out quality assessment, medical audits or utilization review.

Records may be disclosed to health departments and other public health or cooperating medical authorities in connection with program activities and related collaborative efforts to deal more effectively with diseases and conditions of public health significance.

Records may be disclosed to appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

IV. Effects of the Proposed System of Records on Individual Rights

Disclosure may be made to a congressional office from the record of an individual in response to a verified inquiry from the congressional office made at the written request of that individual.

In the event of litigation where the defendant is: (a) The Department, any component of the Department, or any employee of the Department in his or her official capacity; (b) the United States where the Department determines that the claim, if successful, is likely to directly affect the operations of the Department or any of its components; or (c) any Department employee in his or her individual capacity where the Department of Justice has agreed to represent such employee, for example,

in defending a claim against the Public Health Service based upon an individual's mental or physical condition and alleged to have arisen because of activities of the Public Health Service in connection with such individual, disclosure may be made to the Department of Justice to enable that Department to present an effective defense, provided that such disclosure is compatible with the purpose for which the records were collected.

Records may be disclosed by CDC in connection with public health activities to the Social Security Administration for sources of locating information to accomplish the research or program purposes for which the records were collected.

Same as notification procedures. Requesters should also reasonably specify the record contents being sought. An accounting of disclosures that have been made of the record, if any, may be requested.

V. Safeguards

The records in this System are stored in computer tapes/disks, printouts, CD–ROMs, and file folders. The records are retrieved by name and by identification number.

The records in this System have the following safeguards in place to maintain and protect the information as it relates to authorized users, physical and procedural safeguards:

Authorized users—A database security package is implemented on CDC's mainframe computer to control unauthorized access to the system. Attempts to gain access by unauthorized individuals are automatically recorded and reviewed on a regular basis. Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control and Prevention (CDC), or its contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

Physical Safeguards—Access to the CDC Clifton Road facility where the mainframe computer is located is controlled by a cardkey system. Access to the computer room is controlled by a cardkey and security code (numeric keypad) system. Access to the data entry area is also controlled by a cardkey system. The hard copy records are kept in locked cabinets in locked rooms. The local fire department is located directly next door to the Clifton Road facility. The computer room is protected by an automatic sprinkler system, numerous automatic sensors (*e.g.,* water, heat, smoke, etc.) are installed, and a proper mix of portable fire extinguishers is located throughout the computer room. The system is backed up on a nightly basis with copies of the files stored off site in a secure fireproof safe. Security guard service in buildings provides personnel screening of visitors.

Procedural Safeguards—Protection for computerized records both on the mainframe and the CIO Local Area Network (LAN) includes programmed verification of valid user identification code and password prior to logging on to the system, mandatory password changes, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There is routine daily backup procedures and secure off-site storage is available for backup tapes. To avoid inadvertent data disclosure, "degaussing" is performed to ensure that all data are removed from Privacy Act computer tapes and/or other magnetic media. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data.

CDC and contractor employees who maintain records are instructed to check with the system manager prior to making disclosures of data. When individually identified data are being used in a room, admittance at either CDC or contractor sites is restricted to specifically authorized personnel. Privacy Act provisions are included in contracts, and the CDC Project Director, contract officers and project officers oversee compliance with these requirements. Upon completion of the contract, all data will be either returned to CDC or destroyed, as specified by the contract.

Implementation Guidelines: The safeguards outlined above are developed in accordance with the HHS Information Security Program Policy and FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems." Data maintained on CDC's Mainframe and the National Centers' LANs are in compliance with OMB Circular A–130, Appendix III. Security is provided for information collection, processing, transmission, storage, and dissemination in general support systems and major applications.

The records in this System are retained and disposed of in the following way: Records are retained and disposed of in accordance with the CDC Records Control Schedule. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. Source documents for computer are disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed.

VI. OMB Control Numbers, Expiration Dates, and Titles of Information Collection

A. *Full Title:* "Epidemiologic Studies and Surveillance of Disease Problems, HHS/CDC/NCID."

OMB Control Number: 09–20–0136.

Expiration Date: TBD.

VII. Supporting Documentation

A. Preamble and Proposed Notice of System for publication in the **Federal Register**.

B. *Agency Rules:* None.

C. *Exemption Requested:* None.

D. *Computer Matching Report:* The new system does not require a matching report in accordance with the computer matching provisions of the Privacy Act.

[FR Doc. 2010–33017 Filed 1–24–11; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Privacy Act of 1974; Report of Modified or Altered System of Records

AGENCY: Office of Global Program Support Services, Coordinating Office for Global Health (COGH), Department of Health and Human Services (DHHS).

ACTION: Notification of Proposed Altered System of Records.

SUMMARY: The Department of Health and Human Services proposes to alter System of Records, 09–20–0137, "Passport File, HHS/CDC/COGH." HHS is proposing to add the following Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) Memoranda (M) 07–16, Safeguarding Against and responding to the Breach of Personally Identifiable Information:

To appropriate federal agencies and Department contractors that have a need to know the information for the purpose