

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

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 Coordinating Office for Global Health (COGH), Office of Global Program Support Services.

**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 COGH receives comments that would result in a contrary determination.

**ADDRESSES:** You may submit comments, identified by the Privacy Act System of Record Number 09-20-0137:

- *Federal eRulemaking Portal:* <http://regulations.gov>. Follow the instructions for submitting comments.

- *E-mail:* Include PA SOR number 09-20-0137 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:** COGH proposes to alter System of Records, No. 09-20-0137, "Passport File, HHS/CDC/COGH." To show status of passports of CDC employees who travel to foreign countries on official business.

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)*

Coordinating Office for Global Health (COGH)

### Passport File—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. 09-20-0137 "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 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

To show status of passports of CDC employees who travel to foreign countries on official business.

#### II. Authority for Maintenance of the System

Title 5, Government Organization and Employees (5 U.S.C. 301).

#### III. Proposed Routine Use Disclosures of Data in the System.

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.

The Department of Health and Human Services (HHS) may disclose information from this system of records to the Department of Justice, or to a court or other tribunal, when: (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation

or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, the court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected.

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

An individual may learn if a record exists about himself or herself by contacting the system manager at the above address. 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.

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 Coordinating Office for Global Health Local Area Network (LAN) files. The records are retrieved by name.

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 Coordinating Office for Global Health (COGH) personnel and designated support staff of CDC, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

*Physical Safeguards*—The system is backed up on a nightly basis with copies of the files stored off site. Security guard service in buildings provides personnel

screening of visitors. Computer work stations are in a secured area.

**Procedural Safeguards**—Protection for computerized records on the COGH 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. Users of individually identified data protect information from public scrutiny. 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 are 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 the COGH LAN is 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.

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

A. *Full Title:* "Passport File, HHS/CDC/COGH."

*OMB Control Number:* 09-20-0137.

*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. 2010-33018 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 Workforce and Career Development (OWCD), 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, 09-20-0138, "Epidemic Intelligence Service Officers Files, HHS/CDC/OWCD." 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 Office of Workforce and Career Development (OWCD).

**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 OWCD receives comments that would result in a contrary determination.

**ADDRESSES:** You may submit comments, identified by the Privacy Act System of Record Number 09-20-0138:

- *Federal eRulemaking Portal:* <http://regulations.gov>. Follow the instructions for submitting comments.

- *E-mail:* Include PA SOR number 09-20-0138 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:** OWCD proposes to alter System of Records, No. 09-20-0138, "Epidemic Intelligence Service Officers Files, HHS/CDC/OWCD."

The system is designed to process individual applications for the Epidemic Intelligence Service Officer program, and to assess a candidate's suitability for a position in the program.

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)*

*Office of Workforce and Career Development (OWCD)*

#### Epidemic Intelligence Service Officers Files—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. 09-20-0138 "Epidemic Intelligence Service officers Files, HHS/CDC/OWCD." 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.