

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 first routine use permits an individual may learn if a record exists about himself or herself is 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.

A parent or guardian who requests notification of, or access to, a child's medical record shall designate a family physician or other health professional (other than a family member) to whom the record, if any, will be sent. The parent or guardian must verify relationship to the child by means of a birth certificate or court order, as well as verify that he or she is who he or she claims to be.

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, computer tapes/disks, and CD-ROMs.

The records have the following safeguards in place:

*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 nearby. The computer room is protected by an automatic sprinkler system, automatic sensors (e.g., water, heat, smoke, etc.) are installed, and portable fire extinguishers are 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 National Center Local Area Network (LAN) include programmed verification of valid user identification code and password prior to logging on to the system, changed 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 are routine daily backup procedures and secure off-site storage is available for backup files. 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:* These practices are in compliance with 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 CDC's Mainframe and the National Center LAN 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 accordance with the CDC Records Control Schedule. Records are maintained in agency for five years. Disposal methods include erasing computer tapes and 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:* "Studies of Treatment of Tuberculosis and other

Mycobacterioses, HHS/CDC/NCHSTP."

B. *OMB Control Number:* 09-20-0089.

C. *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. 2010-33007 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:** Division of Tuberculosis Elimination, National Center for HIV, STD and TB Prevention (NCHSTP), Centers for Disease Control and

Prevention (CDC), 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, 09–20–0090, “Studies of Testing for Tuberculosis and other Mycobacterioses, HHS/CDC/NCHSTP.” 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 Division of Tuberculosis Elimination, National Center for HIV, STD and TB Prevention (NCHSTP).

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

**ADDRESSES:** You may submit comments, identified by the Privacy Act System of Record Number 09–20–0090:

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

- *E-mail:* Include PA SOR number 09–20–0090 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:** NCHSTP proposes to alter System of Records, No. 09–20–0090, “Studies of Testing for Tuberculosis and other Mycobacterioses, HHS/CDC/NCHSTP.”

To study the diagnostic value of tests used to identify persons infected with *M. tuberculosis* or sensitized by other mycobacteria and persons with active mycobacterial disease. These records may also be used by the Food and Drug Administration in conducting research related to Investigational New Drugs (IND).

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 HIV, STD and TB Prevention (NCHSTP)

### Studies of Testing for Tuberculosis and Other Mycobacterioses—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. 09–20–0090, “Studies of Testing for Tuberculosis and other Mycobacterioses, HHS/CDC/NCHSTP.” 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 study the diagnostic value of tests used to identify persons infected with *M. tuberculosis* or sensitized by other mycobacteria and persons with active mycobacterial disease. These records may also be used by the Food and Drug Administration in conducting research related to Investigational New Drugs (IND).

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

The statutory authority for this system is given under the Public Health Service Act, Section 301, “Research and Investigation” (42 U.S.C. 241).

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

The Privacy Act allows 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 compatible use of data is known as a “routine use”. The routine uses proposed for this System are compatible with the stated purpose of the System:

Test results will be returned to the collaborating physician or responsible hospital official.

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.

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 first routine use permits an individual may learn if a record exists about himself or herself is 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.

A parent or guardian who requests notification of, or access to, a child's medical record shall designate a family physician or other health professional (other than a family member) to whom the record, if any, will be sent. The parent or guardian must verify relationship to the child by means of a birth certificate or court order, as well as verify that he or she is who he or she claims to be.

The following information must be provided when requesting notification: (1) 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, computer tapes/disks, and CD-ROMs.

The records have the following safeguards in place:

*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 nearby. The computer room is protected by an automatic sprinkler system, automatic sensors (e.g., water, heat, smoke, etc.) are installed, and portable fire extinguishers are 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 National Center Local Area Network (LAN) include programmed verification of valid user identification code and password prior to logging on to the system, changed 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 are routine daily backup procedures and secure off-site storage is available for backup files. 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:* These practices are in compliance with 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 CDC's Mainframe and the National Center LAN 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.

Records are retained and disposed of in accordance with the CDC Records Control Schedule. Records are maintained in agency for five years. Disposal methods include erasing computer tapes and 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:* "Studies of Testing for Tuberculosis and other Mycobacterioses, HHS/CDC/NCHSTP."

*OMB Control Number:* 09-20-0090.

*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. 2010-33008 Filed 1-24-11; 8:45 am]

BILLING CODE 4163-18-P