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 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.

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

STORAGE:

Computer tapes/disks and printouts, addressograph plates.

RETRIEVABILITY:

Name and student number are the indices used to retrieve records from this system.

SAFEGUARDS:

1. AUTHORIZED USERS: Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control (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.

2. PHYSICAL SAFEGUARDS: Locked cabinets in locked rooms, 24-hour guard service in buildings, personnel screening of visitors, a limited access, secured computer room with fire extinguishers and overhead sprinkler system, computer terminals and automated records located in secured areas.

3. PROCEDURAL SAFEGUARDS: Protection for computerized records includes programmed verification of valid user identification code, account code and password prior to acceptance of a terminal session or job submission, and frequently changed passwords. Knowledge of individual tape passwords is required to access tapes, and access to systems is limited to users obtaining prior supervisory approval. 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.

4. IMPLEMENTATION GUIDELINES: The safeguards outlined above are developed in accordance with Chapter 45-13, "Safeguarding Records Contained in Systems of Records," of the HHS General Administration Manual, supplementary Chapter PHS.hf: 45-13; Part 6, "Automated Information System Security," of the HHS Information Resources Management Manual; the National Bureau of Standards Federal Information Processing Standards (FIPS Pub. 41 and FIPS Pub. 31).

RETENTION AND DISPOSAL:

Record copy maintained from three to ten years in accordance with retention schedules. Source documents for computer disposed of when no longer needed in the study, as determined by the system manager. Disposal methods include erasing computer tapes and burning or shredding paper materials.

SYSTEM MANAGER(S) AND ADDRESS:

Audio Visual Production Officer, Division of Training and Manpower Development (DTMD), National Institute for Occupational Safety and Health (NIOSH), Robert A. Taft Laboratories, 4676 Columbia Parkway, Cincinnati, Ohio 45226.

NOTIFICATION PROCEDURE:

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 identify 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.

RECORD ACCESS PROCEDURES:

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.

CONTESTING RECORD PROCEDURES:

Contact the official at the address specified under System Manager above, reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

RECORD SOURCE CATEGORIES:

Information is obtained directly from the individual.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

09-20-0089 09-20-0089

SYSTEM NAME:

Studies of Treatment of Tuberculosis and other Mycobacterioses. HHS/CDC/CPS.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Division of Tuberculosis Control, Freeway Office Park, Rooms 145-149, Centers for Disease Control, 1600 Clifton Road, Atlanta, GA 30333and

Federal Records Center, 1557 St. Joseph Avenue, East Point, GA 30344.

A list of contractor sites where individually identified data are currently located is available upon request to the system manager.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Adults and children with tuberculosis or other mycobacterial diseases having been or currently being treated or observed by a limited number of participating local or county health departments, clinics, and hospitals (from 1959 until the present time), including those individuals in selected areas receiving isoniazid therapy or BCG vaccinations, and patients for whom routine tuberculosis treatment is ineffective. Also included are contacts to tuberculosis patients, adults with inactive tuberculosis, and controls.

CATEGORIES OF RECORDS IN THE SYSTEM:

Abstracts of medical data pertaining to clinical trials, including medical history, skin tests, physical examinations, laboratory test results, X-ray results, medications prescribed, smoking habits, etc.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Public Health Service Act, Section 301, "Research and Investigation" (42 U.S.C. 241).

PURPOSE(S):

To determine the effectiveness and safety of a variety of treatments and preventive measures for tuberculosis

and other mycobacterial diseases, to determine the best measures against drug resistant tuberculosis, and to monitor incidence of complications among individuals who have received preventive therapy, including isoniazid.

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

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.

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.

The Department is under contract with private firms for the purpose of collating, analyzing, aggregating or otherwise refining records in this system. Relevant records are maintained by the contractors. The contractors are required to maintain Privacy Act safeguards with respect to such records.

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 Justice Department 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.

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

STORAGE:

Cards, file folders, computer tapes/disks and printouts.

RETRIEVABILITY:

Records are retrieved by the participant's name and/or study I.D. number.

SAFEGUARDS:

1. AUTHORIZED USERS: Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control (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.

2. PHYSICAL SAFEGUARDS: Locked cabinets in locked rooms, 24-hour guard service in buildings, personnel screening of visitors, electronic anti-intrusion devices in effect at the Federal Records Center, fire extinguishers, overhead sprinkler system and card-access control equipment in the computer room, computer terminals and automated records located in secured areas.

3. PROCEDURAL SAFEGUARDS: Protection for computerized records includes programmed verification of valid user identification code, account code and password prior to acceptance of a terminal session or job submission, frequently changed passwords, and Vault Management System. Knowledge of individual tape passwords is required to access tapes, and access to systems is limited to users obtaining prior supervisory approval. When Privacy Act tapes are scratched, a special 'certified" process is performed in which tapes are completely written over to avoid inadvertent data disclosure. 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.

4. IMPLEMENTATION GUIDELINES: The safeguards outlined above are developed in accordance with Chapter 45-13, "Safeguarding Records Contained in Systems of Records," of the HHS General Administration Manual, supplementary Chapter PHS.hf: 45-13; Part 6, "Automated Information System Security," of the HHS Information Resources Management Manual; the National Bureau of Standards Federal Information Processing Standards (FIPS Pub. 41 and FIPS Pub. 31). FRC safeguards are in compliance with GSA Federal Property Management Regulations, Subchapter B—Archives and Records.

RETENTION AND DISPOSAL:

Records are maintained in agency for five years. 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 destroyed by paper recycling process when 20 years old, unless needed for further study.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Tuberculosis Control, Center for Prevention Services, Freeway Office Park, Rm. 111, Centers for Disease Control, 1600 Clifton Road, Atlanta, GA 30333.