

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

Manual files, computer cards, computer tapes/disks, computer listings, microfilm.

RETRIEVABILITY:

Name and case number are the indexes 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, electronic anti-intrusion devices in operation at the Federal Records Center (FRC), 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). 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 three years. Personal identifiers are destroyed as soon as they are no longer necessary for the protection of the individuals involved. 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 Biomedical and Behavioral Science (DBBS), National Institute for Occupational Safety and Health (NIOSH), Robert A. Taft Laboratories, 4676 Columbia Parkway, Cincinnati, Ohio 45226 and

Medical Officer, Division of Standards Development and Technology Transfer (DSDTT), National Institute for Occupational Safety and Health (NIOSH), Robert A. Taft Laboratories, 4676 Columbia Parkway, Cincinnati, Ohio 45226.

Policy coordination is provided by: Director, Office of Program Support, Bldg. 1, Rm. 2011, Centers for Disease Control, 1600 Clifton Road, Atlanta, GA 30333.

NOTIFICATION PROCEDURE:

An individual may learn if a record exists about himself or herself by contacting the appropriate 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.

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.

09-20-0118

SYSTEM NAME:

Study at Work Sites where Agents Suspected of Being Occupational Hazards Exist. HHS/CDC/NIOSH.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Division of Biomedical and Behavioral Science, (DBBS), National Institute for Occupational Safety and Health (NIOSH), Robert A. Taft Laboratories, 4676 Columbia Parkway, Cincinnati, Ohio 45226 and

Federal Records Center, 3150 Bertwynn Drive, Dayton, Ohio 45439.

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

Also, occasionally data may be located at the facilities of collaborating researchers where analyses are performed, data collected and reports written. A list of these facilities is available upon request to the system manager. Data may be located only at those facilities that have an adequate

data security program and the collaborating researcher must return the data to NIOSH or destroy individual identifiers at the conclusion of the project.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Subjects employed at specific sites under study.

CATEGORIES OF RECORDS IN THE SYSTEM:

Occupational history, medical history, results of medical tests including results of hearing tests, demographic data, employee records, psychological and psychometric tests, and data necessary to interpret the medical results.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Occupational Safety and Health Act, Section 20, "Research and Related Activities" [29 U.S.C. 689].

PURPOSE(S):

This system is to determine the relationship between worker exposure to hazardous agents or stressors and occupational disease. This information is used to recommend procedures to reduce the incidence of occupational disease.

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

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.

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.

In the event of litigation initiated at the request of NIOSH, the Institute may disclose such records as it deems desirable or necessary to the Department of Justice to enable the Department to effectively represent the Institute, provided such disclosure is compatible with the purpose for which the records were collected. The only types of litigative proceedings that NIOSH is authorized to request are (1) enforcement of a subpoena issued to an employer to provide relevant information, or (2) contempt citation against an employer for failure to comply with a warrant obtained by the Institute.

Disclosure may be made to NIOSH collaborating researchers (NIOSH contractors, grantees, or other Federal or State scientists) in order to accomplish the research purpose for which the records are collected. The collaborating researchers must agree in writing to comply with the confidentiality provisions of the Privacy Act and NIOSH must have determined that the researchers' data security procedures will protect confidentiality.

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

STORAGE:

Manual files, computer cards, computer tapes/disks, computer listings, microfilm.

RETRIEVABILITY:

Name and case number are the indexes 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, electronic anti-intrusion devices in operation at Federal Records Center (FRC), 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). 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 three years. Personal identifiers are destroyed as soon as the system has stabilized, and statistical summaries can be run. 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 Biomedical and Behavioral Science (DBBS), 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 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.

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 and from employee records.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

09-20-0136

SYSTEM NAME:

Epidemiologic Studies and Surveillance of Disease Problems. HHS/CDC/CID.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Center for Infectious Diseases, Bldg. 1, Rm. 6013, Centers for Disease Control, 1600 Clifton Road, Atlanta, GA 30333

San Juan Laboratories, Center for Infectious Diseases, Centers for Disease Control, San Juan, Puerto Rico 00936

Center for Prevention Services, Freeway Office Park, Rm. 313, Centers for Disease Control, 1600 Clifton Road, Atlanta, GA 30333

Center for Environmental Health, Chamblee Bldg. 27, Centers for Disease Control, 1600 Clifton Road, Atlanta, GA 30333

Epidemiology Program Office, Bldg. 1, Rm. 5009, 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 identifiable data are currently located is available upon request to the appropriate system manager.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Adults and children with diseases and other preventable conditions of public health significance; also included are control group participants.

CATEGORIES OF RECORDS IN THE SYSTEM:

Case reports, medical records, questionnaires, and related documents.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

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

PURPOSE(S):

This record system enables Centers for Disease Control (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.

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

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):

CDC 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 such contractors. Contractors are required to maintain Privacy Act safeguards with respect to such records.

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 identified 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.

Disclosure may be made to a congressional office from the record of