

Disclosure of records or portions of records may be made to a Member of Congress or a Congressional staff member submitting a verified request involving an individual who is entitled to the information and has requested assistance from the Member or staff member. The Member of Congress or Congressional staff member must provide a copy of the individual's written request for assistance.

THE FOLLOWING ROUTINE USES APPLY ONLY TO EEOICPA PROGRAM RECORDS:

Disclosure of dose reconstructions, epidemiologic study records and employment and medical information pertaining to Department of Energy employees and other cancer-related claimants covered under the Energy Employees Occupational Illness Compensation Program Act may be made to the Department of Labor to be used in determining eligibility for compensation payments to such claimants and in defending its determinations under the Act.

Disclosure of personal identifying information associated with cancer-related claims under the Energy Employees Occupational Illness Compensation Program Act may be made to the Department of Energy, other federal agencies, other government or private entities and to private-sector employers to permit these entities to retrieve records required to reconstruct radiation doses and to enable NIOSH to evaluate petitions for inclusion in the Special Exposure Cohort.

Completed dose reconstruction reports for cancer-related claims under the Energy Employees Occupational Illness Compensation Program Act may be released to the Department of Energy and the Department of Labor to permit these entities to fulfill EEOICPA and HHS dose reconstruction regulation requirements to notify claimants of their dose reconstruction results.

Disclosure of personal identifying information associated with cancer-related claims under the Energy Employees Occupational Illness Compensation Program Act may be made to identified witnesses as designated by the Office of Compensation Analysis and Support to assist NIOSH in obtaining information required to complete the dose reconstruction process and to enable NIOSH to evaluate petitions for inclusion in the Special Exposure Cohort.

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

STORAGE:

Manager files, card files, computer tapes/disks and printouts, microfilm, microfiche, and other files as appropriate.

RETRIEVABILITY:

Name, assigned number, plant name, and year tested are some of the indices used to retrieve records from these systems. Other retrieval methods are utilized as individual research dictates.

SAFEGUARDS:

1. *Authorized Users:* A database software security package is utilized to control unauthorized access to the system. Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff or 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:* Hard copy records are kept in locked cabinets in locked rooms (or equivalent safeguarding). Guard service in buildings provides screening of visitors. The limited access, secured computer room contains fire extinguishers and an overhead sprinkler system. Computer terminals and automated records are located in secured areas. Electronic anti-intrusion devices are in operation at the Federal Records Center.

3. *Procedural Safeguards:* Data sets are password protected and/or encrypted. 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 are routine daily backup procedures and Vault Management System for secure off-site storage is available for backup tapes. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data.

Employees and contractor staff 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 government or contractor sites is

restricted to specifically authorized personnel. Privacy Act provisions are included in contracts, and the 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; and part 6, "Automated Information System Security," of the HHS Information Resources Management Manual. FRC safeguards are in compliance with GSA Federal Property Management Regulations, Subchapter B—Archives and Records. Data maintained in CDC Atlanta's Processing Center 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 CIO LANs operate under the current CDC approved version of Novell Netware, and are in compliance with "CDC & ATSDR Security Standards for Novell File Servers."

RETENTION AND DISPOSAL:

Records are maintained in agency for three years after the close of the study. Records transferred to the Federal Records Center when no longer needed for evaluation and analysis are destroyed after 75 years for epidemiologic studies, unless needed for further study. Records from health hazard evaluations will be retained at least 20 years, and then disposed of in accordance with the CDC Records Control Schedule. EEOICPA program records are transferred to the Federal Records Center 15 years after the case file becomes inactive and are destroyed after 75 years. Paper files that have been scanned to create electronic copies are disposed of after the copies are verified. Disposal methods include erasing computer tapes and burning or shredding paper materials.

SYSTEM MANAGER(S) AND ADDRESS:

Program Management Officer, Division of Surveillance, Hazard Evaluations, and Field Studies (DSHEFS), National Institute for Occupational Safety and Health (NIOSH), Robert A. Taft Laboratories, Rm. 40A, MS R12, 4676 Columbia Parkway, Cincinnati, OH 45226.