(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.

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

## STORAGE:

Records are maintained in file cabinets or in computer databases maintained by the RSB and OSHB. Records may be stored in file folders, binders, magnetic tapes, magnetic disks, optical disks and/or other types of data storage devices.

## RETRIEVABILITY:

Records are retrieved by name, Social Security number, office address, or unique RSB or OSHB assigned identification number.

# SAFEGUARDS:

1. Authorized users: Employees who maintain this system are instructed to grant regular access only to RSB/OSHB staff, authorized contractor personnel, U.S. Nuclear Regulatory Commission Inspectors, Radiation Safety Committee Members, Biosafety Committee

members, and other appropriate NIH administrative and management personnel with a need to know. Access to information is thus limited to those with a need to know.

2. Physical safeguards: Rooms where records are stored are locked when not in use. During regular business hours, rooms are unlocked but are controlled by on-site personnel. Individually identifiable records are kept in locked file cabinets or rooms under the direct control of the Project Director.

3. Procedural safeguards: Names and other identifying particulars are deleted when data from original records are encoded for analysis. Data stored in computers is accessed through the use of keywords known only to authorized users. All users of personal information in connection with the performance of their jobs (see Authorized Users, above) will protect information from public view and from unauthorized personnel entering an unsupervised office. The computer terminals are in secured areas and keywords needed to access data files will be changed frequently.

4. Additional RSB technical safeguards: Computerized records are accessible only through a series of code or keyword commands available from and under direct control of the Project Director or his/her delegated representatives. The computer records are secured by a multiple level security system which is capable of controlling access to the individual data field level. Persons having access to the computer database can be restricted to a confined application which only permits a narrow "view" of the data. Data on computer files is accessed by keyword known only to authorized users who are NIH or contractor employees involved in work for the program.

These practices are in compliance with the standards of Chapter 45–13 of the HHS General Administration Manual, supplementary Chapter PHS hf: 45–13, the Department's Automated Information Systems Security Program Handbook, and the National Institute of Standards and Technology Federal Information Processing Standards (FIPS Pub. 41 and FIPS Pub. 31).

# RETENTION AND DISPOSAL:

Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1— "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B–361): Item 1300–B which applies to Division of Safety records. Refer to the NIH Manual Chapter for specific disposition instructions. Radiation exposure records are retained

under item 1300–B–10, which does not allow disposal at this time.

#### SYSTEM MANAGER(S) AND ADDRESS:

Chief, Data and Analytical Services Section, Radiation Safety Branch, DS, ORS, Building 21, Room 104, 9000 Rockville Pike, Bethesda, Maryland 20892.

Chief, Occupational Safety and Health Branch, Division of Safety, National Institutes of Health, Building 13, Room 3K04, 9000 Rockville Pike, Bethesda, Maryland 20892.

#### NOTIFICATION PROCEDURES:

To determine if a record exists, write to the appropriate system manager as listed above.

The requestor must also verify his or her identity by providing either a notarization of the request or a written certification that the requestor is whom he or she claims to be. The request should include: (a) Full name, and (b) appropriate dates of participation.

# RECORD ACCESS PROCEDURE:

Same as notification procedures. Requestors should also reasonably specify the record contents being sought. Individuals may also request an accounting of disclosure of their records, if any.

# CONTESTING RECORD PROCEDURE:

Contact the appropriate System Manager specified above and reasonably identify the record, specify the information to be contested, and state the corrective action sought with supporting documentation. The right to contest records is limited to information which is incomplete, irrelevant, incorrect, or untimely (obsolete).

## **RECORD SOURCE CATEGORIES:**

Information is obtained from the subject individual, previous employers and educational institutions, contractors, safety and health monitoring/surveillance records, employee interviews, site visits, or other relevant NIH organizational components.

# SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

## 09-25-0168

# SYSTEM NAME:

Invention, patent and licensing documents submitted to the Public Health Service by its employees, grantees, fellowship recipients and contractors, HHS/PHS/NIH/OTT.

# SECURITY CLASSIFICATION:

None.