

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

1. Disclosure may be made to a congressional office from the record of a subject individual, in response to an inquiry from the congressional office made at the written request of that individual or his/her representative.

2. Disclosure may be made to Federal, State or local Government entities or to private entities for the purpose of their providing information relevant to medical or legal documentation required for determinations of eligibility or payment, provided that such disclosure is compatible with the purpose for which the records were collected.

3. Disclosure of records may be made to contractors engaged by the Department who need access to the records in order to assist the Department, *e.g.*, expert consultants providing advice on requesters' eligibility for benefits and/or compensation. All such individuals shall be required to maintain Privacy Act safeguards with respect to such records and return all records to HRSA.

4. Disclosure of records may be made to individuals and/or entities as necessary for the purposes of obtaining financial advice and providing benefits and other compensation to requestors approved for payment under the Program. All individuals and/or entities permitted disclosure for this use shall be required to maintain Privacy Act safeguards with respect to such records and return all records to HRSA.

5. Disclosure of records may be made to a Federal agency administering aspects of the Program, as authorized by a Memorandum of Agreement between the Secretary and the head of the Federal agency, or to another Federal agency assisting in the accomplishment of a Departmental function relating to the purposes of this system of records, provided that such disclosure is compatible with the purposes for which the records are collected.

6. Disclosure of records may be made 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 action, if successful, is likely to affect directly the operation of the Department or any of its components; or

(c) Any Department employee in his or her individual capacity where the Department of Justice (DoJ) has agreed to represent such employee, for

example, in defending an action against the Department in connection with such individual, disclosure may be made to DoJ to enable DoJ to present an effective defense, provided that such disclosure is compatible with the purpose for which the records were collected.

7. Disclosure may be made in the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred to the appropriate agency, whether Federal, State or local, charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, rule, regulation or order issued pursuant thereto, provided that such disclosure is compatible with the purpose for which the records were collected.

8. A record may be disclosed for a medical research purpose, only when the Department has determined:

(a) That the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained;

(b) That the research purpose is consistent with the purpose for which the Program was formed;

(c) That the proposed research is scientifically sound in its methods and analyses and is likely to answer the proposed research question;

(d) That the information sought is not available from any other source; and

(e) That the record made available for medical research is redacted of all personal identifiers regarding injured individuals, health care practitioners and employers that are not essential for the accomplishment of the approved research purpose.

(f) The recipient must:

(1) Establish strict limitations acceptable to the Department concerning the receipt and use of any patient-identifiable data;

(2) Establish reasonable administrative, technical, and physical safeguards and/or protocols acceptable to the Department to protect the confidentiality of the data and to prevent the unauthorized use or disclosure of the record;

(3) Remove or destroy the information that identifies an individual at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project; and

(4) Make no further use or disclosure of the record except when required by law.

(a) Further, the Department must secure and approve a written statement attesting to the recipient's understanding of, and agreement to abide by, these conditions of disclosure. Violation of these provisions is subject to penalties set forth under 5 U.S.C. 552a(i)(3) and any other applicable Federal law.

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

Records are maintained in file folders, on computer hard drives and/or disk packs, or in electronic media storage.

**RETRIEVABILITY:**

Retrievability is by name of the requester, and by case number assigned based on the order in which a request form is filed.

**SAFEGUARDS:**

1. Assign Responsibility for Security: Responsibility is assigned to a management official knowledgeable in the nature of the information and process supported by the Smallpox Vaccine Injury Compensation Program (SVICP) request and in the management, personnel, operational, and technical controls used to protect it.

2. Perform Risk Assessment: A risk assessment is to be conducted in conjunction with the development of, and prior to the approval of, the system design and will ensure that vulnerabilities, risks, and other security concerns are identified and addressed in the system design and throughout the life cycle of the project. This is consistent with the HHS Automated Information Systems Security Program Handbook (in particular Chapters V and X).

3. Develop SVICP Request Security Plan: Plan for the adequate security of the SVICP request, taking into account the security of all systems in which the request will operate. SVICP request security plans shall address request rules, training on use of the system, personnel security, contingency planning, technical controls, information sharing, and public access controls.

4. Review SVICP Request Controls: Perform an independent review or audit of the SVICP request security control in accordance with applicable Federal requirements and/or guidelines.

5. Authorize Processing: Ensure that a management official authorizes, in writing, confirmation that the security plan as implemented adequately secures