



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Special Immunization Research System (SIRS)

US Army Medical Command - Defense Threat Reduction Agency (DTRA) Funded System

### SECTION 1: IS A PIA REQUIRED?

**a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

**b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

**SECTION 2: PIA SUMMARY INFORMATION**

**a. Why is this PIA being created or updated? Choose one:**

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

**b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?**

- Yes, DITPR      Enter DITPR System Identification Number
- Yes, SIPRNET      Enter SIPRNET Identification Number
- No

**c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?**

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

**d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?**

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 3013, Secretary of the Army; 10 U.S.C., Chapter 55, Medical and Dental Care; Army Regulation 70-25, Use of Volunteers as Subjects of Research; Army Regulation 70-45, Scientific and Technical Information Program; Occupational Safety and Health Administration Act of 1970; and E.O. 9397 (SSN).

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of this system is to manage the data resulting from clinical research activities that support the unique bio-defense research mission of United States Army Medical Research Institute of Infectious Diseases (USAMRIID). The vision is to serve as the single source of clinical immunogenic data related to all Phase 1 and Phase 2 clinical trails ongoing in the USAMRIID Special Immunization Program (SIP) and the U.S. Army Medical Materiel Development Activity (USAMMDA) Clinical Research Unit. This includes a data entry Graphical User Interface; management of the data, quality control, and data export to biostatisticians. The Special Immunization Research System (SIRS) also facilitates USAMRIID activities to comply with all Federal and Department of the Army regulations and guidelines related to clinical research.

The system collects the following types of PII: Name, Other Names Used, Social Security Number (SSN), Other ID Number, Gender, Race/Ethnicity, Birth Date, Personal Cell Telephone Number, Home Telephone Number, Personal Email Address, Mailing/Home Address, Spouse Information, Medical Information, Employment Information and Emergency Contact.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII collection are unauthorized access, inaccurate information in the system, and unauthorized disclosure of PII. There are security measures in place to mitigate these risks.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.**

**Within the DoD Component.**

Specify.

Authorized personnel within the US Army Medical Research Institute of Infectious Diseases (USAMRIID), US Army Medical Materiel Development Activity (USAMMDA), and military treatment facilities.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

Department of Health and Human Services, if requested.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Some personnel who have access to this system may be employed on a contractual basis. There are clauses in their contracts requiring compliance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) requirements to protect the confidentiality of personal information.

**Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

**Yes**

**No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

During the enrollment phase of each individual protocol, individuals/participants have the opportunity to object to the collection of PII. Individuals read and sign the Privacy Act Statement - Health Care Records, DD Form 2005. A copy of this document is maintained in the individual's medical record. The opportunity to object the collection of their PII is also embedded in the protocol informed consent documents. If an individual/participant does not agree on any portion of the PII collection process they may opt out of participation and this in no way will affect their employment status. No PII would be collected and no information would be entered into SIRS.

(2) If "No," state the reason why individuals cannot object.

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

**Yes**

**No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

During the enrollment phase onto each individual protocol, individuals have an opportunity to give consent to the specific uses of PII. Individuals read and sign the Privacy Act Statement - Health Care Records, DD Form 2005. A copy of this document is maintained in the individual's medical record. The opportunity to object to the specific uses of their PII is also embedded in the protocol informed consent documents. If a individual/participant does not agree on any portion of the PII collection process, they may opt out of participation and this in no way will affect their employment status. No PII would be collected and no information would be entered into SIRS.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other                 | <input type="checkbox"/> None             |

Describe each applicable format.

Individuals are provided the following Privacy Act Statement- Health Care Records, DD Form 2005.

**1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN)** Sections 133, 1071-87, 3012, 5031 and 8012, title 10, United States Code and Executive Order 9397.

**2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED**  
This form provides you the advice required by the Privacy Act of 1974. The personal information will facilitate and document your health care. The Social Security Number (SSN) of member or sponsor is required to identify and retrieve health care records.

**3. ROUTINE USES**  
The primary use of this information is to provide, plan and coordinate health care. As prior to enactment of the Privacy Act, other possible uses are to: Aid in preventive health and communicable disease control programs and report medical conditions required by law to federal, state and local agencies; compile statistical data, conduct research; teach; determine suitability of persons for service or assignments; adjudicate claims and determine benefits; other lawful purposes, including law enforcement and litigation; conduct authorized investigations; evaluate care rendered; determine professional certification and hospital accreditation; provide physical qualifications of patients to agencies of federal, state or local government upon request in the pursuit of their official duties.

**4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION**  
In the case of military personnel, the requested information is mandatory because of the need to document all active duty medical incidents in view of future rights and benefits. In the case of all other personnel/beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED. This all inclusive Privacy Act Statement will apply to all requests for personal information made by health care treatment personnel or for medical/dental treatment purposes and will become a permanent part of your health care record.

Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.

Individuals are also provided a copy of the Notice of Privacy Practices.

**NOTE:**

**Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**