



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Laboratory Information Management System (ELIMS)
---

US Army Medical Command - DHP 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
- New Electronic Collection
- Existing DoD Information System
- Existing Electronic Collection
- Significantly Modified DoD Information System

**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; 5 U.S.C. 7902, Safety Programs; 29 U.S.C. 668, Programs of Federal Agencies; 29 CFR 1910, Occupational Safety and Health Standards; Army Regulation 40-5, Preventive Medicine; E.O. 12223, Occupational Safety Health Programs for Federal Employees; 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 Enterprise Laboratory Information Management System (ELIMS) is a database application and information technology tool required for effective laboratory operations. The US Army Public Health Command (USAPHC) has selected the commercial, web-based tool STARLIMS (Abbott Labs) as the software solution for ELIMS. The STARLIMS software and database offer a set of key features to support all facets of modern laboratory operations. There are three types of laboratory testing which involve PII. One particular analysis performed by the USAPHC labs is the analysis of metal fragment specimens removed from wounded Soldiers. The fragments are sent from US Army Medical Treatment Facilities (MTF) to the USAPHC labs in accordance with US Army and MEDCOM policy. The second type is human clinical bioassay specimens (either urine or fecal) to determine internal radiation dose exposure. The bioassay specimens are from individuals potentially exposed to radioactive materials. The laboratory testing is either for routine exposure monitoring or incident exposure from a radiation source break. The third type of analysis is cholinesterase-testing within the Department of Defense (DoD) Cholinesterase Monitoring Program. The Cholinesterase Monitoring Program ensures proper occupational health monitoring of personnel engaged in chemical agent stockpile and demilitarization operations. All specimens are sent from MTFs or from designated DoD laboratories to the USAPHC labs in accordance with US Army and MEDCOM policy. All data arriving at the USAPHC labs are entered and maintained in the secure, role-based, relational database of the ELIMS. Results from the laboratory analyses are then exported from the system, encrypted locally and electronically transferred back to the respective originating MTF or reported directly by hard copy report and mailed to the originating MTF or respective DoD laboratory.

Categories of individuals collected by the system can include Army active duty, National Guard, Reserve and DoD civilian employees working with radioactive material, chemical agent or pesticides and contract employees with medical monitoring in the terms of their contract.

The types of PII currently collected about individuals include patient name, Social Security Number (SSN) and age. Per DODI 1000.30, Reduction of SSN Use within DoD, USAPHC only uses the SSN for database (computer) matching. Without a common identifier agreed to and implemented by all of the information systems from which USAPHC received data, such as the SSN, the USAPHC does not have a method to inter-relate data received from each of the respective systems.

(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/electronic collection, and unauthorized disclosure of PII. There are administrative, physical, and technical security measures in place to mitigate these risks. The security safeguards are addressed in Section 3d below.

**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.

USAPHC laboratory personnel and US Army Medical Command MTF personnel associated with the analyses described in section 2g(1) above.

**Other DoD Components.**

Specify.

Designated DoD laboratories participating in the Cholinesterase Monitoring Program described in section 2g(1) above.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

Link Solutions, Inc. provide information technology (IT) staff to support USAPHC. These contract employees are required to comply with the Privacy Act and Health Insurance Portability and Accountability Act provisions and complete the following annual mandatory training:

- I. Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) Training.
- II. Information Assurance User Awareness Training.

Contract IT support staff are also required to adhere to: AR 25-2, Information Systems Security; AR 380-5, Information Security program; AR 380-40, Security policy for Safeguarding and Controlling Communications; and DoD Information Assurance Certification and Accreditation Process (DIACAP).

**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.

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

This system does not collect PII directly from the individual. The PII is provided on the document which accompanies the laboratory specimen.

**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.

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

This system does not collect PII directly from the individual. The PII is provided on the document which accompanies the laboratory specimen.

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

**Privacy Act Statement**                       **Privacy Advisory**  
 **Other**     **None**

Describe each applicable format.	<p>This system does not collect PII directly from the individual. The PII is provided on the document which accompanies the laboratory specimen.</p>
----------------------------------	--