



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Medical Library Software (SirsiDynix EOS.Web Medical)

US Army Medical Command - Defense Health Program (DHP) Funded Application

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.

5 U.S.C. 301, Departmental Regulations and E.O. 9397 (SSN), 10 U.S.C. 3013, Secretary of the Army; Pub. L. 106-554, Children's Internet Protection Act; AR 215-1, Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities.

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 SirsiDynix Electronic Online Systems (EOS) Web Medical (EOS.Web Medical) medical library software used to track books and periodical inventories via the check-out and check-in of materials. It is also used to manage access to online mission-critical information. This system provides access to print materials, digital content, and scientific medical journals. Users can search for books and periodicals locally and search medical databases for articles, how-to videos, dosage calculators, and many other topics. The software will be installed and managed locally. The categories of individuals with access to this software includes Federal employees, Federal contractors, and medical students in training programs.

The types of personal information about Federal employees and contractors collected in the system include name, work telephone number, and work email address. The types of personal information collected about about students include name, personal telephone number, and personal email address.

(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 and unauthorized disclosure of PII. There are sufficient administrative, physical, and technical security safeguards in place to mitigate these risks. The specific security measures for this application are addressed in Section 3 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.

PII will be shared with personnel authorized to pursue restitution claims for borrowed property which is lost, damaged, or destroyed.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

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.

The Medical Library has updated the library card registration process to include the ability to consent or object to the collection of the user's PII. The Privacy Act Statement provided in Section 2k below is annotated on the registration form used to collect PII. Individuals objecting to the collection of their PII may use the library resources, but cannot check out library materials without a means to account for this borrowed property.

(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.

The Medical Library has updated the library card registration process to include the ability to consent or object to the collection of the user's PII. The Privacy Act Statement provided in Section 2k below is annotated on the registration form used to collect PII. Individuals objecting to the use of their PII may use the library resources, but cannot check out library materials without a means to account for this borrowed property.

(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 type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The following Privacy Act Statement is annotated on the registration form used to account for borrowed property from the library:

AUTHORITY: 5 U.S.C Section 301 and E.O. 9397.

PRINCIPAL PURPOSES: To account for borrowed property from the library.

ROUTINE USES: To be used by Library staff when contacting borrowers to ensure timely return of property. Information may be released to Comptroller or Judge Advocate claims personnel in order to secure payment for property which is lost, damaged, or destroyed.

MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION: Providing information is voluntary. However, individuals who fail to provide this information can use the library resources but will not be allowed to check-out library materials.

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.