



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Surgery Scheduling System (S3)

Defense Health Agency (DHA)

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. 55, Medical and Dental Care; 32 CFR 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); E.O. 9397 (SSN), as amended.

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 Surgery Scheduling System (S3) is a web-based, automated surgical scheduling system. It provides standardization of Operating Room (OR) scheduling and reporting processes, and allows the collection of enterprise-wide metrics on OR efficiency. S3 is currently in use by 29 Army, 17 Navy, 17 Air Force Military Treatment Facilities (MTFs). S3 provides the electronic version of the following forms: DA Form 4107, Operation Request and Worksheet; DA Form 4108, Register of Operations; and DA Form 7001, Surgery Schedule.

The PII collected and/or maintained in the system includes name, social security number (SSN), race, gender, date of birth and medical information. Information is collected from active duty military, dependents, retirees and/or their dependents, foreign nationals, and former spouses.

S3 is hosted at the DHA Health Information Technology (HIT) Directorate, Infrastructure and Operations (I&O) Division (under Solutions Delivery Division (SDD) Program Management) as a web application on servers housed at select Army, Navy, and Air Force MTFs. S3 does not host a website that is accessible to the public.

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

Privacy risks associated with the PII collected include unauthorized access to PII and inaccurate information entered in the application. Security safeguards are in place to mitigate these risks. There are awareness and training programs, limited physical access, data encryption, and public key infrastructure (PKI) enabled login in order to sufficiently reduce system/application vulnerabilities.

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 is shared among the health care managers within the DHA using this application.

Other DoD Components.

Specify.

PII is shared among the health care managers within each of the Army, Navy, and Air Force MTFs using this application.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

Some contractors supporting the operating room processes at the MTFs have access to PII in S3. Their respective contracts contain language that mandates compliance with the Privacy Act, Health Insurance Portability and Accountability Act (HIPAA) and local policy requirements that protect PII.

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.

Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records, is provided to the patient for review and signature. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel for medical/dental treatment purposes and will become a permanent part of the health care record. If the individual objects to the collection of their PII, comprehensive health care may not be possible, but care is not denied. Individuals can object to the collection of PII in writing.

(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.

Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records, is provided to the patient for review and signature. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel for medical/dental treatment purposes and will become a permanent part of the health care record. If the individual objects to the specific uses of their PII, comprehensive health care may not be possible, but care is not denied. Individuals can object to the collection of PII in writing.

(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.

PII maintained in the S3 information system at an MTF is usually obtained from the MTF's CHCS or other system-to-system transfer. However, if a system-to-system transfer is not available when needed to collect PII for S3, the necessary PII may be collected directly from individuals into a system or records. Therefore, a Privacy Act Statement (PAS) is required whenever PII is collected directly from an individual.

Collection of PII directly from an individual for including in an MTF's S3 system occurs in the MTF environment. Individuals receiving treatment at an MTF, regardless of the MTF's Service affiliation, receive a DD Form 2005, Privacy Act Statement, in connection with registration. Providing DD Form 2005 to an individual in connection with an admission to or registration with an MTF or prior to collection of PII directly from the individual for use in the MTF's S3 system will satisfy the Privacy Act Statement requirement with respect to the occasional need for PII to be collected directly from the individual for use in the S3 system.

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.