



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Omnicell Medication Administration Solution (OMAS)
--

Department of the Navy - TMA DHP Funded System - BUMED
--

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.

SORN authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 1095, Collection from Third Party Payers Act
10 U.S.C. 5131 (as amended)
10 U.S.C. 5132; 44 U.S.C. 3101
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 (SSN) as amended

Other authorities:

Medical and dental care in the DoD are authorized by Chapter 55 of Title 10 U.S.C., section 1071 - 1106. The provision of a pharmacy benefit is part of the medical care benefit.

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.

OMAS is a comprehensive pharmacy management system with a suite of products that a Pharmacy can select from based on their needs.

The OMAS products in use at Navy Medicine are:

1) The OmniCenter Server collects and transfers data from the Omnicell medication dispensing and supply cabinets via the computer network. Database management and administration functions take place at the OmniCenter, allowing authorized users to quickly view and update information about cabinet status.

2) OmniLinkRx automates communication of medication orders and related information between nursing and pharmacy. Nurses place the physician order into an existing digital sending device, scan the order, indicate the processing type (STAT or routine), and the scanned document image is sent to the OmniLinkRx server where it is immediately viewable by pharmacy for order entry. Nurses can check status of those orders to allow them to know when to expect new medications.

3) Pandora VIA provides reporting and analytical functionality around the data collected by bedside point of care and automated dispensing systems (cabinets). The product also offers inventory and patient safety reporting and analysis tools with focus on meeting a Pharmacy's compliance and regulatory need to perform narcotic diversion analysis.

4) Omnicell's SecureVault™ system combines cabinet security with software that enables the pharmacy to trace and monitor the movement of controlled substances along all points in the distribution process. Every transaction is automatically recorded, ensuring a complete audit trail.

The types of personally identifiable information (PII) collected in the system include: patient name, SSN, MRN (Medical Record Number), gender, date of birth, and medical information. The medical information includes patient admit date time and medical information to include diagnosis code (site specific), allergy information, physician name, patient status code (admitted, discharged, pre-admit, temporary), patient weight, patient type, patient room and station. The sponsor's SSN and patient prefix are also collected.

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that OMAS, with its extensive collection of PII, could be compromised.

Because of this possibility, appropriate security and access controls listed in this PIA are in place.

Since OMAS operates on the NMCI Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset.

All systems are vulnerable to "insider threats." Pharmacy managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to the OMAS system. These individuals have gone through extensive background and employment investigations.

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.

OMAS does not collect PII directly from the patient - it is not the source system. The information is used for medical treatment purposes.

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.

DD Form 2005 - Privacy Act Statement - Health Care Records provides:

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.

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.

--

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.