



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Pyxis CII-Safe Medication Storage System
--

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
- 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.

System of Record 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; and, E.O. 9397 (SSN), as amended.

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.

The Pyxis® CII-Safe™ system from CareFusion secures, tracks and monitors the replenishment of controlled substance inventory for both inpatient and outpatient pharmacies in Navy Medical Treatment Facilities (MTF). The Pyxis® CII-Safe™ system brings enhanced value to existing Pyxis® MedStation® system users, providing seamless hospital-wide management of controlled substances. The technology streamlines documentation from the pharmacy to the nursing floor, virtually eliminating time-consuming and error-prone manual record keeping.

The types of PII collected in the system include:

The CII-Safe records raw MedStation transactions in its DB that may include PII and can optionally include the patient name, patient ID and doctors name on orders if manually entered by the pharmacist. This manual entry helps the pharmacy in retrospective review procedures for controlled substance accountability especially when the CII-Safe is used in an outpatient setting and the Pyxis medstation is not deployed for tracking and tracing of medication orders for patients. Normally no patient information is needed for CII-Safe operation as it's function is to respond to stock conditions at the MedStations and not respond to patient requests.

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

Privacy risks would be the release of the patient name, or employee name and potentially the medications that were delivered to that patient. The CII Safe application utilizes bio-metric identification in unison with user name and password to secure any information permitted on the CII Safe system.

The risk(s) would likely come from insider compromise, and the only information the employee would have access to would be the patient information and the user name that was utilized in accessing CII Safe. No user information is accessible by the standard user of CII Safe.

Insider compromises are mitigated by the hiring practices of the US Navy and its military treatment facilities where users can be quickly removed from the CII safe application by authorized personnel.

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.

The authorized pharmacy staff will have access to PII as part of their duties. Vendor authorized personnel will have access to the system to perform support and maintenance.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

DEA

State and Local Agencies.

Specify.

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

Specify.

CareFusion agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information or personally identifiable information that it creates, receives, maintains, or transmits in the execution of their Contracts.

- 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.

Pyxis CII-Safe does not collect PII directly from the patient - it is not the source system.

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.

The information in Pyxis CII-Safe is not collected directly from the individual. The information is sent through a standard interface from CHCS on the local Medical Treatment Facility network. No PII data is required for CII Safe to operate but this data will have to be collected manually and stored the pharmacy staff in a log book or other accounting system used to track and trace controlled substance movement.

The CII-Safe records raw MedStation transactions in its DB that may include PII and can optionally include the patient name, patient ID and doctors name on orders if manually entered by the pharmacist. Normally no patient information is needed for CII-Safe operation as it's function is to respond to stock conditions at the MedStations and not respond to patient requests.

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.

Pyxis CII-Safe does not collect PII directly from the patient - it is not the source 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.