



PRIVACY IMPACT ASSESSMENT (PIA)

For the

CareFusion Pyxis Pharmacy System (CPPS)

Department of the Navy - DHA 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, Health Care Services Incurred on Behalf of Covered Beneficiaries: 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 Social Security Number (SSN), as amended.

42 CFR 290DD Drug and Alcohol Treatment Records
5 CFR 293.502, Subpart E, Employee Medical File System Records
29 CFR Part 5, Labor Standards
5 CFR 339.101-306, Coverage
DoDD 6485.1 Human Immunodeficiency Virus-1 (HIV-1)
DoD 6025.18-R, Health Information Privacy Regulation

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.

The CareFusion-Pyxis Pharmacy System (CPPS), is comprised of multiple components, namely: 1) Pyxis Computerized Unit-Based Inventory Exchange, 2) Medstation 3500, 3) Pyxis Anesthesia System, 4) CIISafe, 5) CareFusion Coordination Engine (CCE) and 6) Pyxis Security Module.

The CPPS is designed to support medication management across the Naval Military Treatment Facilities (MTFs). The system was developed as a turn-key solution to automate specific dispensing functions within hospitals. CPPS provides information management and decision support systems which allow the integration of data and information collected in the local pharmacy.

This system is used to deliver medications to inpatients and is generally not used to support outpatients. Demographic information is required to identify the patient and the medication being prescribed. The intended use of CPPS is to enable medical personnel at various MTFs, and others within the Military Health System (MHS) medical community, to access data captured by the Composite Health Care System (CHCS) and dispense medications according to prescribed physician orders. CPPS processes the extracted data and correlates the information from each of the source databases using a standard set of patient, provider, and other identifiers. CPPS provides a standard clinical interface that allows viewing of a wide range of clinical information pertaining to a single patient or group of patients.

The types of PII collected in the system include: Name, Other Names, SSN, Truncated SSN, Other ID Numbers (Defense Enrollment Eligibility Reporting System (DEERS) identification number and DoD ID Number), Citizenship, Gender, Race/Ethnicity, DOB, Place of Birth, Phone Numbers, Personal Email Address, Mailing/Home Address, Religious Preference, Mothers Maiden Name, Mothers Middle Name, Spouse Information: address, personal phone number, home phone number and Social Security Number; Marital Status, and Emergency Contact.

(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 collected are the unauthorized release of PII data, which can lead to identity theft and fraud.

The patient's name, date of birth, SSN, and medications being prescribed are kept for at least two years on a server and backups within the MTF and according to their site retention policies. Access to this information is limited to medical personnel with a need to know and the servers are kept in secure areas. The backups are either on a sever in the MTFs computer room or if tapes kept in a safe place. All information is protected using user id and password or biometrics.

Host sites or non-CareFusion personnel are not permitted to install patches or other Information Assurance Vulnerability Alert (IAVAs) due to the potential to break the system application functionality, which can result in significant risk to patient health.

The CPPS system is an automated dispensing system supporting decentralized medication management. It utilizes barcode scanning technology to help ensure accurate medication dispensing, and prevents loading of the wrong medication and provides active alerts for an added safety precaution for high risk medications.

Privacy risks would be the release of the patient name, or employee name and potentially the medications that were delivered to that patient. These 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 CPPS.

Insider compromises are mitigated by the hiring practices of the US Navy and its MTFs where users can be quickly removed from the CPPS applications 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 and clinical staff will have access to PII as part of their duties. CareFusion authorized personnel will have access to the system to perform support and maintenance (corrective/preventive). Information is shared with authorized DoD health care providers and managers. PII information will also be shared with MTF physicians, pharmacists, and nurses.

Other DoD Components.

Specify. Information is shared with authorized DoD health care providers and managers. In addition the information may be shared with billing and financial groups within the DoD.

Other Federal Agencies.

Specify. DEA, FDA

State and Local Agencies.

Specify.

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

Specify. CareFusion PII conformance is stipulated in the following contract clauses detailing requirements in accordance with DoD and DoN regulations:

1) 4.12 and 8. Confidentiality; and
2) 13.0 PII and PHI (Subsections: Systems of Record: PIA; Data Use Agreement (DUA); and Privacy Act and HIPAA Training).

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.

CPPS does not obtain information directly from the patient. CPPS receives its data from CHCS and NOT the patient.

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.

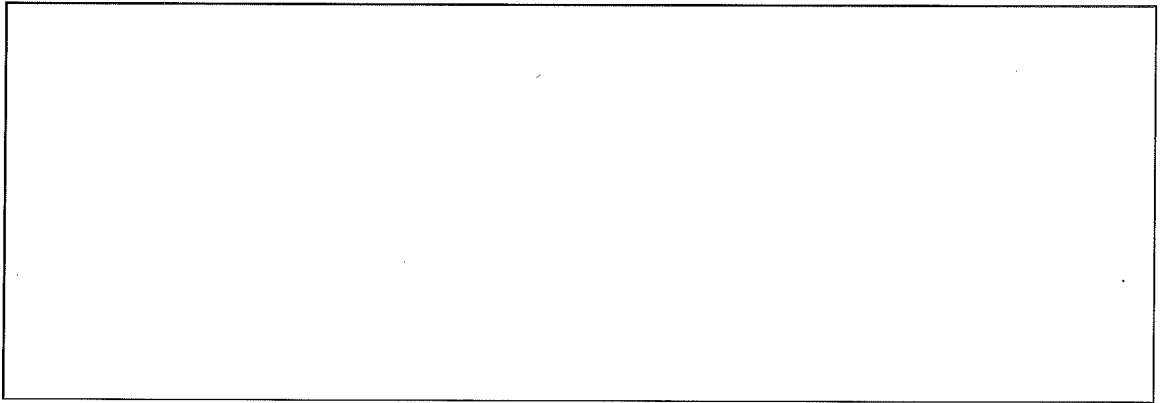
The information in CPPS is not collected directly from the individual. The information is sent through a standard interface from CHCS on the local MTF network.

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.

CPPS 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.