PRIVACY IMPACT ASSESSMENT (PIA)

For the

Omnicell Medication Administration Solution (OMAS)
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**	☐	**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	[Omnicell] OMAS DADMS ID 56025
☐	**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 N06150-2

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; 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; and, E.O. 9397 Social Security Number (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 suite of automation systems that enables Military Treatment Facilities (MTFs) to acquire, manage, dispense, and deliver medications and supplies from the point of entry into the hospital through the central pharmacy, nursing units, operating room, procedural areas, and patient bedsides.

Key components of OMAS are:

1. OmniCenter Server - manages the day-to-day operations of the automated medication and supply dispensing systems throughout a medical facility while giving managers access to essential reports like inventory usage. OmniCenter servers facilitate a single, unified medication database across Omnicell dispensing systems (ColorTouch (CT) Cabinets), from the controlled substance vault (CSM) to Mobile Medication Systems (Savvy) at the bedside. These consolidated and automated processes allow medical and pharmacy staff to focus their time and care on the MTF patients, thus providing more thorough and efficient care.

2. ColorTouch Cabinets - The CT Cabinet is a computerized kiosk system that stores medications and provides a software interface to allow users to gain access to the medications stored in the cabinet.

3. Controlled Substance Management (CSM) - CSM helps pharmacies meet Drug Enforcement Act (DEA) regulations for controlled substance storage, issue, and destruction. CSM provides full accountability of drug movement from the pharmacy to nursing and back to the pharmacy. The control substances can be received, issued, and returned through this application.

4. Central Pharmacy (CP) - CP is a computerized kiosk system which automates the replenishment process for non-controlled medications, providing electronic ordering and receiving as well as expiration date tracking.

5. Savvy Mobile Medication System - The Savvy is a battery-powered workstation on wheels outfitted with locked medication drawers. Nurses can place all needed patient medications for a medication pass into patient-assigned locking drawers and then move from room to room, instead of returning to the automated dispensing cabinet (ADC) between each patient.

6. Pandora Analytics 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.

PII collected about individuals include: patient name, Social Security Number (SSN) , Medical Record Number (MNR), gender, date of birth, and medical information. The medical information includes patient admit date time; 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 Navy Marine Corps Intranet (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 National Agency Check with Law and Credit (NACLC) commensurate with non-critical sensitive positions for which access to sensitive information is required.

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. Omnicell 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. Omnicell authorized personnel will have onsite and remote access to the system to perform support and (corrective/preventive) maintenance. Omnicell PII conformance is stipulated per Central Support Contract (CSC) #N62645-14-F-0013, subsection 5.10. Confidentiality. Contractors and/or service vendors will comply with all applicable Privacy Act requirements, in regards to any personally identifiable information (PII) and protected health information (PHI). Information regarding Privacy Act, PII, and PHI is available to contract personnel for review at the laboratories.

☐ **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.

OMAS 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.

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.

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.