US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/02/2026

OPDIV:

NIH

Name:

CRSS: OPIS: CC Automated Medication Dispensing (Omnicell)

PIA Unique Identifier:

P-1577621-835941

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The PIA has been updated to include all 7 of the Omnicell systems used by the NIH Clinical Center (CC).

Describe the purpose of the system.

The NIH Clinical Center (CC) uses Omnicell to automate medication dispensing, streamlining pharmacy workflows in hospitals by ensuring accurate, secure access to drugs. The modules used include:

Omnicell Automated Medication Dispensing automates the Pharmacy Department's ability to manage and dispense medications at the point of use, increasing patient safety with the use of medication profiles, improving workflow efficiency and enhancing medication security. The system uses secure locked automated dispensing cabinets which allows approved medications to be available to the clinical staff in inpatient care units, in day hospitals and approved clinical locations.

Omnicell SinglePointe automatically assigns medications to patient-specific bins, using guiding lights to assist nurses in retrieval, and eliminates manual bin loading/unloading. The system tracks all medications, including controlled substances stored in secure drawers, and provides a complete audit trail. It reduces medication errors by ensuring profiled orders and automates processes for patient transfers and discharges.

Omnicell Analytics is a web-based software that monitors drug diversion in healthcare facilities by analyzing real-time data from medication transactions. It uses algorithms to identify suspicious usage patterns, comparing individual behaviors to peers and generating user scores for potential diverters. The system provides detailed dashboards tracking medication inventory, stockout rates, and controlled substance transactions across hospital units. It integrates with Omnicell automation systems to streamline compliance and optimize pharmacy operations.

Omnicell Anywhere Registered Nurse (RN) provides a view of the cabinet and the option to remotely access an Omnicell cabinet from any hospital computer or workstation. This feature allows nurses to check medication availability and queue transactions without being physically at the cabinet.

Omnicell Central Pharmacy Manager (CPM) is a software system that automates medication inventory processes in hospital pharmacies, including ordering, receiving, stocking, and dispensing. It integrates with Omnicell's automated dispensing cabinets and other hardware like carousels and packagers to streamline workflows. The system provides real-time visibility into inventory levels, expiration dates, and usage across single or multi-site health systems. It supports compliance with FDA regulations.

Omnicell IVX (6) Workflow is used for safety enhancements in compounding intravenous (IV) drugs in the CC Pharmacy. Omnicell IVX allows tracking medication barcodes, lot/expiration dates, photos of compounding and gravimetric (weight) dose verification.

Omnicell Performance Center is a cloud-based platform that provides real-time analytics and predictive intelligence for hospital pharmacy operations. It tracks medication inventory, usage, and allocation across health systems to reduce waste and optimize stock levels. The system integrates with Omnicell automation tools, offering data-driven insights to manage costs and ensure compliance with FDA regulations. Omnicell Performance Center analyzes the NIH Pharmacy drug inventory and provide guidance on how to optimize the inventory.

Describe the type of information the system will collect, maintain (store), or share.

Omnicell and its modules collect patient information including Name, Date of Birth (DOB), Medical Record Number (MRN), patient demographics (race, ethnicity, sex), patient location, medication notes (including medication order number, name, dosage, route of administration and quantity), allergies, Clinical Research Information System (CRIS) Order identification (ID), and CRIS visit number. Omnicell also collects staff information including name, user role and fingerprint biometric identifier.

The Clinical Research Information System (CRIS) system maintains its own unique PIA on record, including all legal authorities documented.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and

authorize all users and computers in a Windows domain type network assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collects unique user credentials and stores them in an encrypted format. The IAM Service is an essential service which facilitates and governs network access to various resources.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NIH Clinical Center (CC) uses software packages within the Omnicell platform to automate medication dispensing, streamlining pharmacy workflows in hospitals by ensuring accurate, secure access to drugs.

Omnicell Automated Medication Dispensing
Omnicell SinglePointe
Omnicell Analytics
Omnicell Anywhere RN
Omnicell CPM.
Omnicell IVX
Omnicell Performance Center
Omnicell and its modules collect patient information including Name, DOB, MRN, patient demographics, (race, ethnicity, and sex), patient location, medication notes (including medication order number, name, dosage, route of administration and quantity), allergies, CRIS Order ID, and CRIS visit number. Omnicell also collects staff information including name, user role and fingerprint biometric identifier.

The Clinical Research Information System (CRIS) system maintains its own unique PIA on record, including all legal authorities documented.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth
Name
Biometric Identifiers
Medical Records Number
Patient demographics (race, ethnicity, and sex), patient location, medication notes, allergies
CRIS Order ID, CRIS visit number
CC staff user role

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The system uses the personally identifiable information (PII) to track medications dispensed to CC patients and administered by CC clinical staff.

Describe the secondary uses for which the PII will be used.

No secondary uses have been identified.

Identify legal authorities governing information use and disclosure specific to the system and program.

The legal authority to operate and maintain this Privacy Act records system is 42 U.S.C. §§ 241, 248, 282 and 284.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0099 Clinical Research: Patient Medical Records, HHS/NIH/CC.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

Pub. L. Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

The CC and Omnicell have a Memorandum of Understanding (MOU) allowing the remote monitoring of performance data and alerts on the NIH/CC OmniCenter server and remote access capabilities for troubleshooting errors by the Omnicell vendor support engineers.

Describe the procedures for accounting for disclosures.

There are audit logs to allow the system owner to provide that information. There is no sharing of information from Omnicell outside of NIH so accounting for disclosures would not apply.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Every patient voluntarily signs a protocol consent and a general admission consent prior to enrollment into an intramural research protocol and treatment at the Clinical Center. In addition, each patient is provided a formal notification of Information Practices at the Clinical Center and must

certify that they have been so advised.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

General admission and protocol consent forms are signed by each patient. Additionally, an information practices notification form is reviewed and acknowledged in writing by each patient at the time of initial admission to the CC. Enrollment in a clinical research trial is voluntary and the collection of PII and medical notes is necessary to conduct research and provide clinical care.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

All patients are notified of information practices upon admission. Each patient would be advised at the time of the next admission about major system changes and the CC Information Practices Notice would be revised and provided to each patient again.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The CC Department of Clinical Research Informatics (DCRI) Privacy Office will review the complaint and coordinate with the NIH Office of the Senior Official for Privacy (OSOP) to respond to the concern. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC DCRI Privacy Office.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

PII is collected at the time of pre-registration from the patient by the CC Health Information Management Department (HIMD). This PII is validated at the time of admission or registration of the patient in person by the CC Admissions Office and updated or corrected as necessary. PII is also reviewed and updated by the patient during subsequent outpatient clinic visits. Changes/corrections are forwarded to the Admissions Office for updating in CRIS. These practices ensure the data’s integrity, availability, accuracy and relevancy.

Major discrepancies or errors in PII (name, date of birth) are entered in the CC Safety Tracking and Reporting System (STARS), aggregated and reviewed by the HIMD and Admissions management staff with re-training, and system or report modifications made as necessary to prevent errors from recurring.

Information, including PII, is reviewed when queries are performed and data is provided to the clinical research team. Modifications to patient PII such as name, MRN, or medication order number are sent from CRIS to the clinical information systems to keep the patient PII in synchronization across the clinical information systems.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Dual factor authentication with NIH Personal Identity Verification (PIV) card and NIH IAM Services account will occur at time of login to the NIH Network. System owners are responsible for creating the proper security groups within their systems with the applicable permissions for group members to enforce least privilege.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

Describe training system users receive (above and beyond general security and privacy awareness training).

Application specific training is provided to CC Pharmacy Department staff and to CC Nursing Department staff prior to the creation of Omnicell system accounts.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item I-0006: Clinical Care Services Records
These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule.
Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff. (DAA-0443-2012-0007-0006)

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Physical controls: The information technology (IT) hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from public networks to prevent unauthorized or malicious access. Access to the system is controlled by NIH login which authenticates the user prior to granting access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity

and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.