US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/23/2025

OPDIV:

IHS

Name:

Pyxis Automated Dispensing System IHS

PIA Unique Identifier:

P-1459344-963286

The subject of this PIA is which of the following?

Major Application

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?

New

Does the system have Security Authorization (SA)?

No

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

Describe the purpose of the system.

Pyxis is an Automated Dispensing Cabinet (ADC) medication storage system used in IHS facilities to enhance patient safety, safely store, track and dispense medications, reduce delays, support regulatory compliance, prevent drug diversion, improve hospital workflow, and facilitate quality assurance.

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

Upon check-in or admission, Pyxis receives patient data from the IHS Resource Patient Management System (RPMS) system to support accurate medication dispensing and tracking. RPMS is the system the hospital utilizes for patient record management. Information from RPMS via the IHS Pharmacy interface is transmitted to Pyxis. RPMS is cover under a separate PIA.

The system allows two-way communication for sharing drug usage data, which is stored for 90 days before it is overwritten and archived locally (IHS on-site server) for regulatory compliance, which requires data be available for a minimum of 2 years. No data is sent off-site.

The Pyxis system receives patient demographic, clinical, and visit information—such as name, date of birth, sex, medical record number, allergies, and admission/discharge details—from the IHS system to ensure accurate medication access and patient safety. It uses IHS Active Directory (cover under a separate PIA) for user authentication and may include biometric fingerprint verification, which is converted to a secure algorithm and not stored. This data ensures secure access, prevents diversion, and supports continuity of care as patients move through the facility

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

pon check-in or admission, Pyxis receives patient data from the IHS Resource Patient Management System (RPMS) system to support accurate medication dispensing and tracking. RPMS is the system the hospital utilizes for patient record management. Information from RPMS via the IHS Pharmacy interface is transmitted to Pyxis. RPMS is cover under a separate PIA.

The system allows two-way communication for sharing drug usage data, which is stored for 90 days before it is overwritten and archived locally (IHS on-site server) for regulatory compliance, which requires data be available for a minimum of 2 years. No data is sent off-site.

The Pyxis system receives patient demographic, clinical, and visit information—such as name, date of birth, sex, medical record number, allergies, and admission/discharge details—from the IHS system to ensure accurate medication access and patient safety. It uses IHS Active Directory (cover under a separate PIA) for user authentication and may include biometric fingerprint verification, which is converted to a secure algorithm and not stored. This data ensures secure access, prevents diversion, and supports continuity of care as patients move through the facility.

Name, date or birth, sex, and medical record number is utilized to identify the correct patient when selecting medications and to help avoid errors related to similar names. Visit information is collected to assure patients' Pyxis profiles are displayed at the appropriate Pyxis device closest to their location of care. Admission, discharge, and transfer information is utilized to assure the patient's Pyxis profiles follow them as they move throughout the facility during their course of care. User biometric information is collected to maintain secure access and prevent diversion by password theft or sharing.

As part of the vendor contract, all Pyxis parts, whether leased or purchased, that may contain patient information are turned over to the IHS site prior to decommissioning and shipping devices back to Pyxis.

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 demographic, clinical, and visit information, sex, and fingerprint

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

Employees
Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is primarily utilized to provide direct patient care, meet regulatory requirements, and prevent or detect controlled substance diversion detection or prevention. User PII in the form of user credentials and biometric identifiers are collected to control system access.

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

Secondary uses of the PII in the Pyxis system include inventory management and medication error investigation.

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

Departmental Regulations (5 U.S.C. 301); Privacy Act of 1974 (5 U.S.C. 552a); Federal Records Act (44 U.S.C. 2901); Section 321 of the Public Health Service Act, as amended (42 U.S.C. 248); Section 327A of the Public Health Service Act, as amended (42 U.S.C. 254a); Snyder Act (25 U.S.C. 13); Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.); and the Transfer Act of 1954 (42 U.S.C. 2001-2004). IHS Manual Part 3 - Chapter 7

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.

09-17-0001 Medical, Health, and Billing Records Systems

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

Not applicable

Is the PII shared with other organizations?

No

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

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of PHI and of the individual's rights and IHS' legal duties with respect to PHI. A copy of the Notice is provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office provides a copy of the current Notice to the patient. The staff member has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed "Acknowledgment of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record.

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.

Pyxis is not the source system and does not collect personal information directly from individuals. RPMS handles data collection and is responsible for providing opt-out options for PII.

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

Pyxis is not the source system and does not collect personal information directly from individuals. RPMS handles data collection and is responsible for notifying and obtaining consent from the individual.

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.

All complaints are addressed to the Service Unit Chief Executive Officer or (his or her) designee for investigation. Complaints are documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Complaints may also be filed directly with the Secretary, Department of Health and Human Services (DHHS).

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

Pyxis is not a source system and does not have a process in place to review PII. Personal information is not collected directly from individuals. RPMS handle data collection and is responsible for periodically reviewing PII/PHI within its system to ensure data integrity, availability, accuracy, and relevance

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.

Pyxis access is linked to IHS Active Directory profiles and requires pharmacy approval for user privileges. Supervisors request access via ServiceNow and SailPoint, and the pharmacy grants the minimum necessary permissions based on job roles and responsibilities.

ServiceNow and SailPoint are covered under s separate PIA.

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.

The system utilizes least privilege and role-based access controls. Access is granted to a limited number of authorized administrators, developers, direct contractors, and federal employees. When a user's IHS Active Directory account is suspended or terminated, all Pyxis access is automatically blocked. Roles for users are determined by the principle of 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.

Role-based training, IHS Rules of Behavior agreements, HIPAA and Privacy training, and Information System Security and Privacy Awareness training courses are required to be completed annually by all IHS users.

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

Department specific training reiterates expectations and importance of HIPPA compliance and login security to avoid password sharing. Use of Biometric access is a Pyxis functionality the facility may utilize to prevent password sharing.

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.

Transitory Records - DAA-GRS2017-0003- 0001

Transitory records are routine records of short term value (generally less than 180 days). Pyxis data is only stored on the Pyxis server for 90 days before it is overwritten. Archiving of Pyxis data for regulatory compliance is critical and is setup by local IT to have the Pyxis server data save the required information to local servers. Records retention is governed by IHS Manual Part 5 Chapter 15.

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

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.

Technical Controls: IHS firewalls, IT governance on site. 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.

Physical Controls: The IT hardware used to host protected information is located in a secured IHS 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."