US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/14/2024

OPDIV:

NIH

Name:

CRSS: Investigational Drug Management System

PIA Unique Identifier:

P-8465617-626085

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.

This validation is intended to refresh content and update the security authorization date. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The NH Clinical Center (CC) Investigational Drug Management System (IDMS) is used by the Pharmacy Department to create, manage and store data related to investigational drugs used in the CC. The Investigational Drug Management and Research Section (IDMRS) provides investigational drug services for Institutional Review Board (IRB) approved intramural research protocols. IDMS provides IDMRS with the ability to track the inventory of the investigational drugs and the raw materials used to make the drugs. The system also provides the ability to fill prescriptions from the inventory of investigational drugs tracked by IDMS. Additionally, it provides Protocol/Study tracking for compliance with protocol requirements.

The IDMS system receives patient and prescription order data from the Clinical Research Information System (CRIS), the CC electronic health record. CRIS maintains its own approved privacy impact assessment (PIA) on record, including all legal authorities documented.

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

IDMS collects patient information (name, medical notes, date of birth, CRIS order number and Medical Records Number), prescribing physician's name, and research protocol information (protocol number and patient study number). The IDMS system receives patient and prescription order data from the CRIS, the CC electronic health record. The information is stored permanently to satisfy clinical research and Food and Drug Administration (FDA) requirements. CRIS maintains its own approved 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 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.

IDMS is a custom application that tracks ordering, dispensing and administration of investigational medications to CC patients enrolled on NIH IRP protocols. The IDMS system receives patient and prescription order data from the CRIS, the CC electronic health record. The information is stored permanently to satisfy clinical research and FDA requirements. CRIS maintains its own approved privacy impact (PIA) on record, including all legal authorities documented.

IDMS collects patient information (name, medical notes, date of birth, CRIS order number and Medical Records Number), prescribing physician's name, and research protocol information (protocol number and patient study number).

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
Medical Records Number
Medical Notes
Patient Study Number, CRIS Order Number
Research protocol number and patient study number).
Prescription order data

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 primary purpose of the personally identifiable information (PII) is to associate investigational medication actions such as ordering and administration with a specific CC patient and meet regulatory compliance requirements.

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

There have been no secondary uses specified by the system owner.

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, NIH Clinical Research: Patient Medical Records

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Public 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.

Not applicable. The study monitors and auditors do not directly access IDMS and their data collection does not include uniquely identifying information.

Describe the procedures for accounting for disclosures.

If a request for an accounting is received, IDMS has audit logs which would allow the system owner to provide that information. Specifically, a log of reports generated for purposes of FDA compliance and NIH IRP study compliance is recorded in IDMS.

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.

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. Therefore, a patient may not opt out of the collection or use of their PII while participating in research at the CC.

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 Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.

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

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. Study monitors review PII and investigational drug administration records for compliance with protocol requirements. CC pharmacists review the CRIS orders containing PII when filling prescriptions. All discrepancies are reported to and investigated by the IDMS User Administrator. The CC IDMRS runs routine accountability audit reviews.

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.

Access to PII is assigned to personnel based upon their role and current job responsibilities.

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. Authentication with NIH Personal Identity Verification (PIV) card 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. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

IDMS has application specific training for users

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 03-001: 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-0443-2019-0001-0001

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

Physical Controls: The 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 default commodity public networks to prevent unauthorized or malicious 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.