US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/07/2025

OPDIV:

NIH

Name:

CC CRIS DataMart

PIA Unique Identifier:

P-4422147-810115

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 system was upgrade in accordance with the CRIS upgrade in April 2024. The vendor, Allscripts, was purchased by Altera Digital Health and may occasionally be referenced as Altera.

Describe the purpose of the system.

The NIH Clinical Center (CC) Clinical Research Information System (CRIS) DataMart is a repository of a copy of all CRIS data used for institute extractions and for clinical reporting. CRIS Production data is replicated in real time to DataMart where Biomedical Translational Research Information System (BTRIS) and Rehabilitation Medicine Department (RMD) administrators can pull data into their respective systems by extract, transform, and load (ETL) processes. ETL provides the method of moving the data from various sources into a data warehouse. The Department of Research Informatics (DCRI) team also pulls information for authorized CC reports and dashboards presented to CC leadership. CRIS DataMart shares PII with BTRIS and RMD for research purposes and both are CC systems. There is no sharing outside of NIH. CRIS, RMD, and BTRIS maintain their own

unique PIAs, with all legal authorities documented.

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

Patient information collected includes name, medical record number (MRN), Mother's maiden name, e-mail address, phone numbers, medical notes, date of birth, mailing address, device identifiers, radiologic images, social security number (SSN), health insurance information, medical notes including chief complaint, allergies, medical orders, consents, clinical documentation including periodic assessments of height, weight, vital signs, pain, intake and output, medications administered and services provided. Examples include results of laboratory tests, imaging studies, blood product utilization, social work encounters, medical & ethical consults, surgery, device identifiers and other related clinical interactions while a patient at the Clinical Center.

NIH staff PII collected includes name, user identification (ID), role, NIH Enterprise Directory (NED) ID, email address, phone number, Institute or Center (IC). The National Provider Identifier number, a unique 10 digit identification number issued to healthcare providers in the US by the Centers for Medicare and Medicaid, is also stored for authorized users in the prescriber role.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including 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 collect unique user credentials and stores them in an encrypted format. The IAM Services are 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) Clinical Research Information System (CRIS) DataMart is a repository of a copy of all CRIS data used for institute extractions and for clinical reporting. CRIS Production data is replicated in real time to DataMart where Biomedical Translational Research Information System (BTRIS) and Rehabilitation Medicine Department (RMD) administrators can pull data into their respective systems by extract, transform, and load (ETL) processes. ETL provides the method of moving the data from various sources into a data warehouse. The Department of Research Informatics (DCRI) team also pulls information for authorized CC reports and dashboards presented to CC leadership. CRIS DataMart shares PII with BTRIS and RMD for research purposes and both are CC systems. There is no sharing outside of NIH. CRIS, RMD, and BTRIS maintain their own unique PIAs, with all legal authorities documented.

Patient information collected includes name, medical record number (MRN), Mother's maiden name, e-mail address, phone numbers, medical notes, date of birth, mailing address, device identifiers, radiologic images, social security number (SSN), health insurance information, medical notes including chief complaint, allergies, medical orders, consents, clinical documentation including periodic assessments of height, weight, vital signs, pain, intake and output, medications administered and services provided. Examples include results of laboratory tests, imaging studies, blood product utilization, social work encounters, medical & ethical consults, surgery, device identifiers and other related clinical interactions while a patient at the Clinical Center.

NIH staff PII collected includes name, user identification (ID), role, NIH Enterprise Directory (NED) ID, email address, phone number, Institute or Center (IC). The National Provider Identifier number, a unique 10 digit identification number issued to healthcare providers in the US by the Centers for Medicare and Medicaid, is also stored for authorized users in the prescriber role.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM)

Services which maintains its own unique privacy impact assessment (PIA) on record, including 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 collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

Yes

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

Social Security Number
Date of Birth
Name
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Names include patients, care providers, users and referring physicians. User credentials include User ID, role, NED ID, IC.
Radiologic images, Health Insurance identifiers, National Provider Identifier number, 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?

100,000-999,999

For what primary purpose is the PII used?

The PII is used primarily for clinical research.

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

No secondary purposes 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 the OPDIV

Other HHS OPDIV

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

N/A. Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

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.

Every patient must sign a protocol consent and authorization for the collection of PII prior to enrolling in 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 acknowledge 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.

Information is obtained from patient interviews, medical notes from referring physicians that are provided by the patient, a multi-disciplinary care team, and diagnostic, therapeutic, and research results. 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. 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 and acknowledge the notification in writing. 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. 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.

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.

The users (employees and direct contractors) accessing PII complete an electronic CRIS Access Request Form (eCARF) requesting a CRIS DataMart account, listing their role and privileges needed to perform their job responsibilities. The eCARF is approved by the CC Chief Information Officer (CIO). Access is granted by the DCRI SCM DBA Lead. Appropriate CRIS training is completed before a CRIS DataMart account is activated.

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 in DCRI, BTRIS and RMD.

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.

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

Senior technical users in DCRI, BTRIS and RMD provide on-the-job training for new hires granted access to CRIS DataMart from their respective departments. CRIS DataMart users must also complete CRIS training.

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 Intramural Records Retention Schedule.

Item I-0006: Clinical Care Services Records
(DAA-0443-2012-0007-0006)
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: TEMPORARY. Cut off annually at end of fiscal year. Destroy 7 years after cutoff.

Item I-0010: Patient Medical Records
(DAA-0443-2012-0007-0010)
These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study.
Disposition: TEMPORARY. Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference.

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

Infrastructure supporting the system is located in the CC or Center for Information Technology (CIT) datacenter that is on a Federal government campus, protected by armed guards, and behind secured doors where all entry and exit is tracked, monitored, and restricted to authorized individuals only (monitoring is 24/7).

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 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.

Remote access to this system is permitted via NIH VPN or Clinical Center Citrix. These systems maintain their own unique PIAs.

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.