US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/30/2025

OPDIV:

NIH

Name:

CC CRIS Insurance Tab

PIA Unique Identifier:

P-8320028-003909

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.

There have been no significant changes since the last assessment was done. The assessment is updating the authorization date.

Describe the purpose of the system.

The Clinical Research Information System (CRIS) Insurance Tab is a custom tab that supports Admissions processes to collect information related to a patient's health insurance and scan their health insurance card.

The insurance information is stored in CRIS and available to Admissions staff, Health Information Management Department (HIMD) staff and Social Work Department (SWD) staff and CRIS Prescriber staff (read only). The information is accessed to facilitate Clinical Center (CC) patient transfers to an outside hospital or to coordinate discharge planning where health insurance information is requested.

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

The CRIS Insurance Tab stores the patient's personally identifiable information (PII). Name, date of birth (DOB) and medical record number (MRN) are derived from CRIS tables. Additional patient insurance information collected include: Insured's Name (may be different from patient), Relationship to Patient, Insurance Name, Insurance Type, Policy Number, Group Number, Insurance Phone Number, Effective Date and Expiration Date. Secondary Insurance information, including Insurance Name, Insurance Type, Policy Number, Group Number, Insurance Phone Number, Effective Date, and Expiration date may also be collected. Scanned images of the patient's insurance card and photo identification (ID) are also collected.

Users requiring access 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 usernames and passwords (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 Insurance Tab is located within CRIS. After selecting the patient in CRIS, Admissions staff open the tab and follow steps to scan the insurance card and photo ID. The insurance information is displayed in discrete fields, verified with the patient and saved. If the patient has a secondary insurance, Admissions staff repeat the scanning and verification process. Once saved, the information is stored permanently. If insurance coverage changes, the information may be edited by staff in Admissions, HIMD and SWD. The tab includes print functionality for approved users. No other CRIS users can access the Insurance Tab.

Users requiring access 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 usernames and passwords (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.

Date of Birth
Name
Photographic Identifiers
Phone Numbers
Medical Records Number
Financial Accounts Info
Insured's name and relationship to patient,
Insurance Name, Type, Policy number, Group number, Insurance phone number
Effective Date, Expiration Date

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

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 care.

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
Hardcopy
Email
Online
Other
Government Sources
Within OpDiv
Other HHS OpDiv
State/Local/Tribal
Other Federal Entities
Non-Government Sources
Public

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.

N/A

Describe the procedures for accounting for disclosures.

The system owner will work with the application administrator to review audit logs to identify persons accessing the requesting individual's information. Tracking the recipient and purpose of PII disclosures to an outside party is a manual process for CRIS. The Health Information Management Department's Medicolegal Request Tracking System track's authorized disclosures to patient or parties outside of NIH for patients in CRIS.

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.

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.

Patients may choose not to provide health insurance information with no impact on their participation in research.

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 account, listing their role and privileges needed to perform their job responsibilities. The eCARF is approved by their supervisor and appropriate CRIS training is completed before a CRIS 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 Admissions, HIMD and SWD.

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).

Role-based CRIS user training includes how to look up a patient, identification of physicians, enter orders, view and retrieve results, view reports, enter clinical documentation and generally utilize the information in their role as healthcare providers and research staff. Classroom and/or on-line training is completed before obtaining a user account.

Superusers in Admissions provide on-the-job training for new hires to train them how to access, scan, verify and save information in the CRIS Insurance Tab. Superusers in HIMD and SWD provide on-the-job training for new hires in their respective departments.

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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: The IT hardware and software used to host the protected information 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. Personnel accessing these systems use privileged and separate accounts for administrative access to systems.

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