US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/29/2016

OPDIV:

NIH

Name:

Clinical Research Information System

PIA Unique Identifier:

P-1293848-693120

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?

Yes

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 NIH Clinical Center Patient Portal was launched in July 2013. Patient Portal is a secure website designed to provide registered patients with access to key medical information from CRIS regarding care received at the CC including test results.

Describe the purpose of the system.

The Clinical Research Information System (CRIS) supports clinical care, collects data for research, and supports hospital operations. CRIS supports the diverse functions required to provide clinical care to CC patients and facilitate the collection of NIH intramural research program (IRP) protocol requirements. Examples include, admissions, transfers, discharges; entering orders for services to be performed on CC patients such as administering medications, performing laboratory tests, radiology exams and blood transfusions; documenting the patient assessments by physicians, nurses, and other clinical care providers and making those documents, test results and reports viewable to physicians in order to make decisions about their care and response to clinical research activities.

CRIS supports hospital operations that include Hospital Information Management, Pharmacy, Admissions, Laboratory, Radiology, Blood Bank, Nursing, Respiratory, Nutrition, Social Work, Spiritual Ministry and Surgery.

There are more than 1,000 active intramural research protocols in CRIS. The research covers a variety of health issues such as cancer, eye disease and visual disorders, heart, lung and blood diseases, genome research, age-related disease and disabilities, alcohol-related issues, infectious, immunologic and allergic diseases, arthritis, musculoskeletal and skin disease, hearing and speech disorders, craniofacial-oral-dental diseases, diabetes, endocrine, kidney disorders and obesity, mental illness, and neurological disorders.

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

Information collected related to patients include 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), 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, and other related clinical interactions while a patient at the Clinical Center.

Information collected on family member's listed as next of kin, include name, relationship and phone number. For minors, the next of kin may include a biological parent, a legally authorized adoptive parent or legal guardian. In each case, the name, relationship and phone number is collected. Information collected related to authorized users include name, userID, role, NIH Enterprise Directory Identity Number, email address, phone number, Institute or Center.

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

CRIS is an electronic health record which collects PII and sensitive medical information. CRIS displays relevant information such as patient's demographics, medical history, medical orders, test results, clinical documentation and medications administered to authorized users. Access to a specific patient's relevant medical information enables healthcare providers and clinical research team to assess the patient's condition and make appropriate clinical care and research decisions. CRIS shares the patient demographics, patient location and medical orders with clinical department information systems for processing. The clinical department information systems shares the report of completed medical orders with CRIS. Examples of the clinical department information systems include Laboratory Information System, Radiology Information System, Perioperative Information System, Nutrition System, Admissions, Transfer and Voucher Request System, Automated Medication Dispensing System, Outpatient Pharmacy System, Sunrise Medication Management System and Respiratory Information System.

CRIS collects sensitive information such as the user ID and the workstation name in order to control access and track the activities performed by the user, i.e., entering an order, documenting a note or printing a report.

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

Provider physician name and location, radiologic images which include name and MRN as

Names include patients, next of kin/legal guardian for minors, care providers, users and referring physicians

Examples of medical notes include chief complaint, allergies, medical orders, consents, clinical documentation, height, weight, vital signs, pain assessments, intake and output, medications, services provided, laboratory test results, imaging studies, blood products administered, medical consults, surgery, and other clinical interventions while a patient at the Clinical Center.
User credentials include User ID, role, NIH Enterprise Directory Identity Number, email address, phone number, Institute or Center.

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

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 patient treatment.

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

The PII is also used for research. The PII and medical notes attributed to an NIH approved research protocol are made available to the principal investigator, research team and auditors for analysis.
The PII is also used for training. The NIH Clinical Center's Clinical Electives Program offers clinically oriented rotations to senior medical and dental students. The NIH Clinical Research Nursing Residency Program trains the newly licensed graduate nurse transitioning from nursing school to professional practice and a career in clinical research nursing.

Describe the function of the SSN.

SSN is used for identification in order to process patient travel requisitions and report patient reimbursements to the Internal Revenue Service.

Cite the legal authority to use the SSN.

In addition, Executive Order 9397 (8 Fed. Reg. 16,094 (Nov. 30, 1943)) as amended by Executive Order 13478 (73 Fed. Reg. 70,239 (Nov. 20, 2008) (http://www.fms.treas.gov/tinpolicy/background.html).

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; E.O. 13478, Executive Order 9397 (8 Fed. Reg. 16,094 (Nov. 30, 1943)), asamended by, Executive Order 13478 (73 Fed. Reg. 70,239 (Nov 20, 2008)).

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, Patient Medical Records, HHS/NIH/CC

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

In progress

Is the PII shared with other organizations?

Yes

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

Within HHS

PII is shared with NIH Biomedical Translational Research Information System (BTRIS) and several NIH IRP research systems for analysis by the research teams. NIH IRPs receiving PII from CRIS include; National Cancer Institute, National Eye Institute, National Heart Lung and Blood Institute, National Institute of Allergy and Infectious Diseases, National Human Genome Research Institute and National Institute of Diabetes and Digestive and Kidney Diseases.

Other Federal Agencies

SSN is shared with NIH Business System (NBS) to facilitate payment and reimbursement to patients. NBS shares the SSN with Internal Revenue Service as taxable income received by the patient.

Private Sector

PII is securely disclosed to outside organizations under contract with the CC to provide hospital services that include medical transcription, laboratory testing and scheduling appointment for CC patients. PII is also shared with any physician authorized by the patient to receive a summary of the patient's care.

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

PII is disclosed so that Clinical Center services such as medical treatment may be provided to patients. Information Sharing Agreements (ISA) or Memorandums of Understanding (MOU) document the disclosures within HHS and outside of HHS.

Describe the procedures for accounting for disclosures.

If a request for an accounting is received, there are audit logs to allow the system owner to provide that information.

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 voluntarily execute a protocol consent and authorization prior to entry onto 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.

Information is obtained from patient interviews, medical notes from referring physicians that are provided by the patient, a data feed from the hospital scheduling system, 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. 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.

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 Occurrence Reporting System, 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.

Users:

Clinical care and research.

Administrators:

Clinical care and research. System development and maintenance.

Developers:

System development and maintenance.

Contractors:

Clinical Care and research. Development, investigation of technical issues and maintenance

Others:

Auditors for research data validation.

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

The users (employees and contractors), and auditors accessing PII complete a CRIS Access Request Form (CARF) requesting a CRIS account, listing their role and privileges needed to perform their job responsibilities. The CARF is approved by their supervisor and appropriate CRIS training is completed before a CRIS account is activated. There are 115 user roles based on the user's business functions such as prescriber, nurse, admissions staff, audiologist, dentist, genetic counselor, laboratory technician, medical student, medical records staff, pharmacist, and social worker. Administrators and developers (employees and contractors) may be exposed to PII incidental to the performance of development, investigation of technical issues and maintenance activities. The administrators and developers are provided access by the System Administrator which is limited to the purposes specific to their role.

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.

All personnel must complete all NIH Privacy and Security training before access is granted and annual refresher training to maintain access.

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

Clinical Research Information System user training includes how to look up a patient, their physician, 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 on-line training is completed before obtaining a user account. Periodic training updates are provided to active users when application enhancements are implemented throughout the year and annually with application version upgrades.

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 Retention Schedule. Clinical Care Services Records, DAA-0443-2012-0007-0006, and are temporary records that can be destroyed seven years after cutoff. Patient Medical Records, DAA-0443-2012-0007-0010, are temporary records that can be destroyed after five years of inactivity or when no longer needed for scientific reference. Radiology and imaging Records, DAA-0443-2012-0007-0007, are temporary records that can be destroyed 60 years after inactivity.

Refer to the schedule for descriptions of each type of record and for the complete disposition instructions:

https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-health-and-human-services/rg-0443/daa-0443- 2012-0007_sf115.pdf.

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

PII is secured according to NIH Enterprise Information Security Plan (EISP). The EISP specifies the security controls needed to secure and protect PII with administrative, technical, physical and privacy controls. Authentication with NIH PIV cards will occur at the time of login to the CC network and via Computer Application Service Provider Resource (CASPER) for remote application users. PII is secured using user names/passwords, least privilege, separation of duties, an intrusion detection system, firewalls, locks, badge access to NIH campus and background investigations. This meets all National Institute of Standards and Technology Special Publications (NIST SP) and Federal Information Security Management Act (FISMA) requirements. If an application or system is unable to meet the security requirements, then a Plan of Actions and Milestones (POA&M) is created or NIH Waiver is requested from the NIH Chief Information Officer (CIO).