# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

03/08/2024

### OPDIV:

NIH

### Name:

CRIS : Clinician Portal (Referring Clinician Portal)

**PIA Unique Identifier:**

P-7416922-402996

**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 Clinician Portal (Referring Clinician Portal) now includes user account information collected from outside regulatory auditors/monitors.

**Describe the purpose of the system.**

The Clinical Research Information System (CRIS) Clinician Portal, also known as the Referring Clinician Portal, is a web-based application that allows authorized referring clinicians access to their patient's medical records. The Clinician Portal also provides referring and Clinical Center (CC) clinician(s) to exchange pertinent status updates related to patients receiving care in and out of the NIH. The system is also used by regulatory auditors/monitors to access pertinent information in order to conduct audits of research studies.

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.

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

Referring clinicians and regulatory auditors/monitors request access to the NIH CC Clinician Portal via a website (https://clinicianportal.cc.nih.gov). The website collects personally identifiable information (PII) that is used to create a user self-service account for logging in to the CRIS Clinician Portal. This includes:
National Provider Identifier Number (NPI)
Name
Work Email Address
Work Phone Number
Work Fax Number
Work Address
Medical Practice Name
Username and Password

CC Health Information Management Department (HIMD) administrators validate that the referring clinician has been authorized by the patient to receive labs and reports.

The CRIS Clinician Portal stores the referring clinician and auditor/monitor user's email and password for purposes of authenticating approved users upon login. Patient data (name, medical record number (MRN), test results, exams and clinical documentation) are stored and maintained in CRIS and only displayed in the Clinician portal. CRIS maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented.

NIH users requiring administrative access log in using the NIH Identity, Credential, and Access Management Services (IAM), which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in an encrypted format. The IAM 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.**

The CRIS Clinician Portal, also known as the Referring Clinician Portal, is a web-based application that allows authorized referring clinicians access to their patient's medical records. The Clinician Portal also provides referring and CC clinician(s) to exchange pertinent status updates related to patients receiving care in and out of the NIH. The system is also used by regulatory auditors/monitors to access pertinent information in order to conduct audits of research studies.

CRIS supports the diverse functions required to provide clinical care to CC patients and facilitate the collection of IRP protocol requirements.

Referring clinicians and regulatory auditors/monitors request access to the NIH CC Clinician Portal via a website (https://clinicianportal.cc.nih.gov). The website collects personally identifiable information (PII) that is used to create a user self-service account for logging in to the CRIS Clinician Portal. This includes:
NPI
Name
Work Email Address
Work Phone Number
Work Fax Number

Work Address
Medical Practice Name
Username and Password

CC HIMD administrators validate that the referring clinician has been authorized by the patient to receive labs and reports.

The CRIS Clinician Portal stores the referring clinician and auditor/monitor user's email and password for purposes of authenticating approved users upon login. Patient data (name, MRN, test results, exams and clinical documentation) are stored and maintained in CRIS and only displayed in the Clinician portal. CRIS maintains its own unique PIA on record, including all legal authorities documented.

NIH users requiring administrative access log in using the NIH IAM, which maintains its own unique PIA on record, including 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.**

Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
National Provider Identifier (NPI), Medical Practice Name
Patient test results, exams and clinical documentation
Username and password

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

Public Citizens
Patients
Clinicians referring patients to NIH for clinical research

**How many individuals' PII is in the system?**

<100

**For what primary purpose is the PII used?**

To verify and validate the referring clinician or auditor's identity in order to establish a CRIS Clinician Portal account.

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

There are no secondary uses 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

Online

Government Sources

Within the OPDIV

Non-Governmental Sources

Public

Private Sector

**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?**

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.**

The NIH CRIS Clinician Portal Privacy Notice is posted on the website and describes the personal information. Per the Privacy Notice, the information collected is used solely to verify the clinician's identity in order to establish a Clinician Portal account.

**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.**

Referring clinicians may not provide their PII for login access. Their patient(s) may request a copy of their personal medical information be sent to the clinician's mailing address.

Regulatory auditors/monitors must use the CRIS Clinician Portal in order to perform official monitoring duties for their company. Otherwise they cannot perform the necessary tasks.

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

The CRIS Clinician Portal will notify individuals when major system changes occur by posting a revised Privacy Notice on the website.

**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 reviewed periodically by the CC HIMD staff. CC HIMD implement patient requests to add or modify physicians authorized to access their medical records via the CRIS Clinician Portal.

**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 granted to referring clinician users based on their request and the authorization of their patients.

Access to PII is granted to regulatory auditor/monitor based on meeting the requirements stated in the HIMD Regulatory Audit Guide.

Access to PII is assigned to CC HIMD administrators and direct contractors and authorized by CC HIMD Leadership using NIH IAM.

**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. Administrative access is limited to authorized employees based on current roles. Authentication with NIH Personal Identity Verification (PIV) card and NIH IAM account. 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.

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

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

A link on the website provides Instructions on how to use the Clinician Portal for training of referring clinicians. Supplemental application training is also available by CC HIMD staff.

CC HIMD Leadership provide on the job training for new administrators and new direct contractors.

**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 03-005: Patient Medical Records.
These records document admissions and medical treatment for a patient accepted in a research project.
Disposition: Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference. DAA-0443-2012-0007-0010

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

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 refreshers. Personnel accessing these systems use privileged and separate accounts for administrative access to systems.
Remote access to this system is through a Virtual Private Network (VPN) gateway, named the Clinical Center Computer Application Service Provider Resource (CC CASPER) which meets all National Institute of Standards and Technology Special Publications (NIST SP) and Federal Information Security Management Act (FISMA) requirements.

Note: web address is a hyperlink.