US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/01/2025

OPDIV:

NIH

Name:

CRIS: Secure Health Message (SHM)

PIA Unique Identifier:

P-1730845-318918

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 the security authorization date. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The Clinical Research Information System (CRIS) Secure Health Message (SHM) is a web-based tool within CRIS for sending and receiving secure electronic communications between Care Providers, and Care Providers and patients with active FollowMyHealth accounts. As part of business operations, the physicians, research nurses and Health Information Management Department (HIMD) often communicate with patients who are not in the hospital about upcoming appointments, admissions and test results. Similarly, patients often have questions for their research team in between visits. SHM provides an encrypted mechanism for sending messages containing personally identifiable information (PII) and sensitive information (SI). Additionally, SHM includes an option to append messages to a patient record.

CRIS supports the diverse functions required to provide clinical care to Clinical Center (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 Clinical Center (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 Care and Surgery.

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 Clinical Center (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 Care and Surgery.

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

CRIS SHM Web-App uses the following employee and patient information from CRIS:
Name (CareProvider and patient)
Email Address (CareProvider and patient)
Medical Notes
Date of Birth
Medical Records Number
Message contents

This information is collected, stored and/or maintained through the Clinical Research Information System (CRIS), which maintains its own approved Privacy Impact Assessment (PIA), and follows security procedures to secure the platform, and all PII, using administrative, technical, and physical controls.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 usernames and passwords (user credentials) and stores them in an encrypted format. The IAM is an essential service which facilitates and governs network access to various resources.

As part of CRIS, SHM Web-App utilizes the CRIS application infrastructure for creating and sending messages to the FollowMyHealth Patient Portal. FollowMyHealth is a patient portal offered by the National Institutes of Health Clinical Center to its patients. FollowMyHealth is provided by a third-party, Veradigm LLC. Allscripts is responsible for the portal's operation and security, and Veradigm terms-of-use govern the use of the portal. The information in CRIS is stored permanently. Patients manage information in their FollowMyHealth account once it is sent from CRIS. They may choose to remove information, but that does not remove it from the source application (CRIS). A Memorandum

of Understanding (MOU) between Veradigm FollowMyHealth (FMH) and the NIH Clinical Center Department of Clinical Research Informatics' (DCRI) Clinical Research Information System (CRIS) authorizes the information sharing between the CRIS system and the FollowMyHealth patient portal.

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

The Clinical Research Information System (CRIS) Secure Health Message (SHM) is a web-based tool within CRIS for sending and receiving secure electronic communications between Care Providers, and Care Providers and patients with active FollowMyHealth accounts. As part of business operations, the physicians, research nurses and Health Information Management Department (HIMD) often communicate with patients who are not in the hospital about upcoming appointments, admissions and test results. Similarly, patients often have questions for their research team in between visits. SHM provides an encrypted mechanism for sending messages containing personally identifiable information (PII) and sensitive information (SI). Additionally, SHM includes an option to append messages to a patient record.

CRIS SHM Web-App uses the following employee and patient information from CRIS:
Name (CareProvider and patient)
Email Address (CareProvider and patient)
Medical Notes
Date of Birth
Medical Records Number
Message contents

This information is collected, stored and/or maintained through the Clinical Research Information System (CRIS), which maintains its own approved Privacy Impact Assessment (PIA), and follows security procedures to secure the platform, and all PII, using administrative, technical, and physical controls.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 usernames and passwords (user credentials) and stores them in an encrypted format. The IAM is 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
E-Mail Address
Medical Records Number
Medical Notes

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 primary purpose for the employee information is to associate the Care Provider's messages with name and NIH email address.

The primary purpose for the patient information is to associate messages with the patient's email address and account in FollowMyHealth and to attach messages to CRIS records if necessary.

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

There are no secondary uses.

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

Government Sources

Within the OPDIV

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.

An MOU between Allscripts FollowMyHealth and the NIH CC DCRI CRIS authorizes the information sharing between the CRIS system and the FollowMyHealth patient portal.

Describe the procedures for accounting for disclosures.

The CC Health Information Management Department (HIMD) has the ability to generate reports from the system to monitor and report on the sender and recipient of messages, when messages were sent, and whether they were attached to patients' CRIS records. These reports also enable the HIMD to generate an accounting of disclosures report as necessary.

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 in to 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. Patients may establish a FollowMyHealth account and use the SHM features after viewing the Allscripts Terms of Use and Privacy Policies online. Additionally, patients give consent for NIH CC to share portions of their medical record with Allscripts LLC® to populate their FollowMyHealth portal account as part of the NIH CC Authorization for Electronic Communications and Communication with Outside Healthcare Providers form.

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 in CRIS while participating in research at the CC. Patients may choose not to enroll in the FollowMyHealth patient portal and use other options for secure communication with their providers. CRIS accounts utilize the NIH IMS account of the authorized CareProviders. CareProviders may not opt out of the information collection as it is a requirement for the creation of an NIH email.

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 CC 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.

The CC Health Information Management Department has the ability to generate reports from the system to monitor and report on the sender and recipient of messages, when messages were sent, and whether they were attached to patients' CRIS records.

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.

Employee and direct contractors are provided access to PII as part of their CRIS account. NIH CC Health Information Management Department and Medical Executive Committee have approved giving SHM to all active Care Providers in CRIS.

Patient users are provided access after giving consent on the NIH CC Authorization for Electronic Communications and Communication with Outside Healthcare Providers form.

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.

Access to PII is assigned based on the user's role and job responsibilities. The role-based security model allows administrative users access across all Service team configurations or access to only the Service team configurations affiliated with their Institute/Center (I/C). 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 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).

Patients are provided a user guide and frequently asked questions which are available on the NIH CC's patient information website.

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

Care Providers receive training to configure their mailbox, create and respond to messages as part of CRIS Website 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.

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 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 training and awareness 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.