US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/30/2025

OPDIV:

NIH

Name:

CRIS Sunrise Mobile App

PIA Unique Identifier:

P-6208118-609639

The subject of this PIA is which of the following?

Electronic Information Collection

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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 point of contact and authorization date.

Describe the purpose of the system.

Sunrise Mobile (referred to as CRIS Mobile) is a mobile application (app) that is fully integrated with the NIH Clinical Center (CC) Clinical Research Information System (CRIS) and extends the use to mobile devices.

CRIS Mobile enables physicians and nurses to immediately benefit by having detailed patient data with them whenever they need it, wherever they are on mobile devices (tablets and smartphones) that are enrolled in the NIH Mobile Device Management (MDM) system. Its role-based approach lets physicians and nurses manage their daily activities.

CRIS Mobile offers key clinical information via a user's MDM-managed mobile device. Specific features available with initial implementation include order and order set entry, viewing of results and electronic medication administration records (eMAR).

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

CRIS Mobile will collect user information when authenticating to the application. User information collected includes user name and password, passcode, device information such as workstation identification (ID), device name, and internet protocol (IP) address and acknowledgement of the Altera Sunrise Mobile end user app agreement (EUAA). The information will be stored in the Sunrise Mobile application at the NIH CC. User information may also be stored by the vendor, Altera Sunrise Mobile.

CRIS Mobile will collect patient information as well. The patient information is limited to patient photographs. The patient photos collected using the device's camera will be stored in existing CRIS databases, and displayed within the CRIS application

CRIS Mobile will enable users to view patient information stored in CRIS, specifically name, medical record number (MRN), patient photo, if provided, and related medical notes such as allergies, medications, orders, results, and vital signs.

CRIS Mobile users authenticate to the app with their CRIS username and password. Users may store credentials in the app for ease of use during a single session. If a user stores credentials in the app, the user must create a 6-digit passcode, which must be entered to reauthenticate when the app locks after the timeout session.

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.

CRIS has undergone a security assessment and maintains an approved PIA. NIH Mobile Device Management, operated by NIH CIT, has undergone a security assessment and maintains their own approved PIA.

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

Sunrise Mobile (referred to as CRIS Mobile) is a mobile application (app) that is fully integrated with the NIH Clinical Center (CC) Clinical Research Information System (CRIS) and extends the use to mobile devices.

CRIS Mobile enables physicians and nurses to immediately benefit by having detailed patient data with them whenever they need it, wherever they are on mobile devices (tablets and smartphones) that are enrolled in the NIH Mobile Device Management (MDM) system. Its role-based approach lets physicians and nurses manage their daily activities.

CRIS Mobile offers key clinical information via a user's MDM-managed mobile device. Specific features available with initial implementation include order and order set entry, viewing of results and electronic medication administration records (eMAR).

CRIS Mobile will collect user information when authenticating to the application. User information collected includes user name and password, passcode, device information such as workstation identification (ID), device name, and internet protocol (IP) address and acknowledgement of the Altera Sunrise Mobile end user app agreement (EUAA). The information will be stored in the Sunrise Mobile application at the NIH CC. User information may also be stored by the vendor, Altera Sunrise Mobile.

CRIS Mobile will collect patient information as well. The patient information is limited to patient photographs. The patient photos collected using the device's camera will be stored in existing CRIS databases, and displayed within the CRIS application

CRIS Mobile will enable users to view patient information stored in CRIS, specifically name, medical record number (MRN), patient photo, if provided, and related medical notes such as allergies, medications, orders, results, and vital signs.

CRIS Mobile users authenticate to the app with their CRIS username and password. Users may store credentials in the app for ease of use during a single session. If a user stores credentials in the app, the user must create a 6-digit passcode, which must be entered to reauthenticate when the app locks after the timeout session.

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.

CRIS has undergone a security assessment and maintains an approved PIA. NIH Mobile Device Management, operated by NIH CIT, has undergone a security assessment and maintains their own approved PIA.

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

Yes

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

Name
Photographic Identifiers
Device Identifiers
User name and password, passcode
IP address

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?

500-4,999

For what primary purpose is the PII used?

The primary purpose for staff PII is to authenticate users to the mobile application. In addition, IMS credentials are used for authentication to the CRIS system and attribution of orders, medication administration and records viewed by individual CRIS users.

The primary purpose for device information is used for identification of workstation accessing CRIS and audit logs.

The primary purpose for the patient PII is positive patient identification in the electronic medication administration record (eMAR) feature.

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

The CC CRIS Mobile administrators anticipate the analysis of user PII for performance improvement activities.

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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Other

Government Sources

Within the DOC

Non-Government Sources

Public

Not Applicable

Identify the OMB information collection approval number and expiration date

No OMB collection approval number is not needed as CRIS Mobile only requires the PII of federal employees and direct contractors for internal use only.

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?

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.

NIH has a Memorandum of Understanding (MOU) with Allscripts, the application vendor. The Allscripts MOU will be updated to include CRIS Mobile.

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. The CRIS Mobile audit logs reveal a user's access to CRIS from their mobile device. The CRIS application audit logs together with CRIS Mobile audit logs would reveal the patient medical records viewed through CRIS Mobile.

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 Altera vendor provides a process for notification. When a user logs in, the application will display the CRIS Mobile Privacy Notice and provides users with a choice to Accept or Decline. The user acknowledgment is tracked in the audit log tables.

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.

CRIS Mobile extends the use of CRIS for clinicians who choose to use it on their government furnished managed mobile devices. The collection of limited PII is necessary for authentication of users and secure connection of registered devices to the CRIS system. If users object to the information collection, they may continue to access CRIS from registered workstations and laptops on the NIH network.

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

Users will be notified of the information collection practices through an online privacy notice upon access to CRIS Mobile. The online privacy notice would be revised and presented to users if major system changes impact the uses of their PII.

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.

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. The system produces reports for review by CRIS Mobile system administrators and CRIS database administrators.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the CRIS system, allowing users only access to the minimum amount of PII necessary to perform their job. The security permission to access CRIS Mobile will be added to the active CRIS account for clinicians such as physicians, dentists, nurse practitioners, physician assistants and nurses. Additionally, CRIS Mobile users must have active CRIS account and must be on the NIH mobile device management tools.

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.

Determinations are made based on role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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).

The CRIS Mobile training focuses on requirements for using the application on a user's mobile device and how to log in. The requirements include:
NIH mobile device management tools installed on the phone
Sunrise Mobile installed on the phone
Active CRIS account

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

Training is accomplished by reviewing power point instructions. Once logged in to Sunrise Mobile, the presentation and navigation of patient records is very similar to CRIS so additional training is not required.

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 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. CRIS Mobile utilizes the technical controls enforced on smartphones by the NIH Mobile Device Management tools.

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.