US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/05/2025

OPDIV:

NIH

Name:

CRSS: Safety Tracking and Reporting System

PIA Unique Identifier:

P-3777562-566285

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 PIA has been updated to meet the requirements of Executive Order - Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.

Describe the purpose of the system.

The Safety Tracking and Reporting System (STARS) is for reporting unexpected events: events that happen in or around the hospital including those that happen to patients; this could name patients and could include a medical record number (MRN). The system has a function to anonymize event participants, de-identifying personally identifiable information (PII), for reporting purposes.

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

STARS can collect staff name, patient name, medical record number (MRN), date of birth (DOB), sex, residential address, phone, room number at the Clinical Center, location of the event, protocol, primary physician, admission date, protocol number, and medical notes. Type and nature of event. Allergies are also collected. A user may enter data in a narrative box. The name of a witness could

also conceivably be included in that box.

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 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 collects unique user credentials and stores them in an encrypted format. The IAM Service 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.

STARS is for reporting unexpected events: events that happen in or around the hospital including those that happen to patients. The system has a function to anonymize event participants, de-identifying PII for reporting purposes.

STARS can collect staff name, patient name, MRN, DOB, sex, residential address, phone, room number at the Clinical Center, location of the event, protocol, primary physician, admission date, protocol number, and medical notes. Type and nature of event. Allergies are also collected. A user may enter data in a narrative box. The name of a witness could also conceivably be included in that box.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with 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.

Date of Birth
Name
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
protocol and number, sex
Location of event and location at the Clinical Center, primary physician, admission date, Allergies

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?

Investigation, performance improvement, report tracking, logging, review for accuracy and patient safety. It can only be accessed by providers in the Clinical Center (CC) or the NIH Institutes and Centers (ICs).

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

There are no secondary uses specified by the system owner.

Identify legal authorities governing information use and disclosure specific to the system and program.

The legal authority to operate and maintain this 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

In-Person

Government Sources

Within the DOI

Identify the OMB information collection approval number and expiration date

An OMB collection approval number is not needed as STARS only uses the PII of federal employees for internal use only.

This system is also exempt from an OMB Information Collection Number through Public Law 114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the Paperwork Reduction Act 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.

Neither an Information Sharing Agreement (ISA) nor a Memorandum of Understanding (MOU) is required at the CC level for this system.

Describe the procedures for accounting for disclosures.

Procedures for accounting - will vary from system to system:
If a request for an accounting is received, there are audit logs to allow the system owner to provide that information.
Accounting for disclosures requires both automated and manual processes to compile in systems containing PII. Disclosure to others by the party accessing that information is a manual process, and this may be a formal manual process (tracked with a spreadsheet, for example) or an ad-hoc process (tracked after the fact, only upon request, using information such as notes or emails). There is no one tracking system in place that is in common use for all systems.

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 and varies for each application.

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.

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.

Reports are used to confirm the integrity and consistency of data stored in the system. In-application dashboards are also used to provide visibility of data and continuous monitoring.

Availability: Backups for the servers and databases are performed on a consistent basis.

Accuracy: Accuracy is confirmed by way of reporting as well as joining against the EHR database for comparison and validation.

Relevancy: Monitored by way of reports from the system as well as system change requests from users to continue adapting the system to better meet users needs.

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 assigned to personnel based upon current job responsibilities. A system administrator must first permit an NIH employee to have rights to the application. Then they are able to log in using the NIH IAM Services. NIH IAM maintains its own PIA, including all legal authorities documented.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy 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).

Application specific one-on-one peer training is provided as needed.

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 03-001: 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 07-201 - Systems and data security records.
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

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.

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.