US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/28/2016

OPDIV:

AHRQ

Name:

Quality and Safety Review System (QSRS)

PIA Unique Identifier:

P-2659132-468506

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The QSRS system supports a consistent measure of patient safety that encompasses virtually all causes of patient harm to hospital inpatients. Specifically, the system collects data on existing adverse event measures and on additional types of adverse healthcare events to provide accurate data on the overall rate of harm from inpatient hospital care. The system supports a more efficient measurement of patient safety and enhanced reporting via compliance and consistency with AHRQ's Common Formats. Common Formats are event data reports that are designed for use during hospitalizations and this information contains data regarding unsafe conditions based on audits of patient charts. The data provides insight and identifies trends on patient safety in United States hospitals by performance at the national level and through local use efforts that highlight localized patient safety problems.

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

The QSRS system collects and permanently stores data on existing adverse event measures of patients and on additional types of adverse events to provide more accurate data on the overall rate of harm from inpatient hospital care.

Collected information includes medical notes, medical record numbers, gender, race, admission and discharge dates, attending and operating healthcare providers, date of death, and medical procedure codes. Information collected from direct contractors and employees that support the system include a username and password to provision access to the system for system maintenance and development.

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

The QSRS system supports a medical record abstraction process that permits the collection, analysis, and reporting of specified patient safety and quality of care data. The data captured in QSRS is determined by an algorithm based on AHRQ's Common Formats and abstracted by the Centers for Medicare and Medicaid Services (CMS) from medical records stored in their systems. The output from the algorithm helps determine if a patient safety event occurred or not. This data, in aggregate form, is utilized by CMS for their quality programs.

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

Medical Records Number

Medical Notes

Hospital Federal Tax ID

Gender/Race/Ethnicity

Admission/Discharge Dates

Attending/Operating Physicians

Diagnosis/Procedures Codes/Date of Death/ User Credentials

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

Employees

Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

QSRS utilizes PII for the purposes of collecting aggregate data to perform analysis on patient medical records and to identify patient safety incidents and examine those incidents thoroughly. The ultimate goal of using PII is to develop a surveillance system that reports on adverse patient safety events that affect the patient and to improve overall standards of in patient care. PII collected from employees and direct contractors is used to provision system account access for system development and maintenance.

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

N/A

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

Section 934(c) of the Public Health Service Act (PHS Act) (42 U.S.C. 299c-39c).

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.

SORN is In Progress

Identify the sources of PII in the system.

Other

Government Sources

Other HHS OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

N/A

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.

No notice is provided by AHRQ for the collection or use of the PII, as the data is not gathered from individuals directly. The medical records are selected based on hospitals identified by Centers for Medicare & Medicaid Services (CMS). PII collected is not used to make determinations about an individual that affect care or the approval or denial of a benefit. AHRQ employees and direct contractors are aware of the requirement to collect user credentials prior to the provisioning of account access for system development and maintenance activities.

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.

Individuals cannot opt out of the collection of their information because records are selected by an algorithm for the purpose of identifying trends of adverse care at a national level. The information is not used to make a determination about an individual and is collected to identify the situational consequence of a particular type of care. AHRQ employees and direct contractors must provide user credentials to access the system to perform their roles as system developers and administrators.

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

An algorithm is used to collect patient information for the purpose of identifying the particular circumstance or result of treatment. PII is collected about the specific point of care and therefore PII collected describes characteristics of an individual at a point in time. There are no determinations made about an individual based upon the collection of PII and any major changes to the system will not influence the data collected during the point of care or treatment of the individual. AHRQ employees and direct contractors are made aware at the time of any major changes that affect the provisioning of account access and must change a password or log-in information to regain access to the system.

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.

An algorithm is used to collect patient information for the purpose of identifying the particular circumstance or result of treatment. PII is collected about the specific point of care and therefore PII collected describes characteristics of an individual at a point in time. There are no determinations made about an individual based upon the collection of PII. AHRQ employees and direct contractors are made aware at the time of any major change that affects the provisioning of system account access, and must change a password or log-in information to regain access to the system.

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 within the system is not used to make determinations about individuals. The accuracy, availability, relevancy, and integrity of the collected data is assumed correct when entered by the abstractor. As a result, there is no process to review the PII. There are no periodic reviews of credentials other than a review of the roles associated with user to ensure that users only have access to the system when required, and that access is terminated once the role is complete.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

AHRQ users will access the QSRS system to view reports on patient event data in order to perform analysis and quality assurance on the surveillance event data.

Administrators:

Administrators: Database Administrators (DBA) will access the QSRS server/databases (DB) in order to perform; database server builds, implementation of QSRS builds into production environments, DB patch management, DB maintenance, DB indexing, DB re-builds, adhoc queries, etc.

Contractors:

Direct AHRQ contractors that support Clinical Data Abstraction Center (CDAC) Medical Record Abstractors to input data. AHRQ Users to review reports, and QSRS DBAs to QSRS perform analysis, etc.

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

All accounts follow secure user account management based on "least privilege" for their access. Each role is created to ensure that only the information needed to perform their job duties will be accessed in the system. System Administrators (SA's) do not have any access to any patient level PII. Database Administrators (DBA's) have unique accounts established that only allow for normal database maintenance activities, i.e., patch management, security, design, maintenance. DBA's have access to patient level PII as part of their role in record maintenance; indexing, rebuilds & debugging. Developers do not have access to any patient level PII. Developers utilize test data that is sanitized of any patient level PII.

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.

Each role in the system is established based on a "least privilege" account access methodology. Each role created in the system account directory is setup to only allow the entitlements and rights to see the PII data required.

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.

Standard AHRQ Information Systems Security Awareness & Training (SAT) is required for all new users to the system via MS PowerPoint and before access is granted. AHRQ SAT is then required every 365 days as part of the annual recertification process. AHRQ requires all users to read and sign a "Certification of Completion" at the end of the SAT that is submitted for approval to the AHRQ Security and Privacy Team prior to providing access to the system as part of the SAT process.

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

N/A

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.

No records schedule currently exists for this system. Records will be maintained until a records schedule has been identified.

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

The following controls are in place:

Administrative Controls include but are not limited to: Policies and Procedures; Information Security, Badge, Incident Response, Information Security and Privacy Rules of Behavior, Physical and Environmental, Record Retention, Initial, Annual and Role based security training, and Background checks.

Technical Controls that are in place, include, but are not limited to: USERID/Passwords, 2-Factor Authentication, Access Control Lists (ACL), Data and Internet Encryption, Network and Host Based Firewalls, Network Intrusion Detection/Prevention Systems (IDS/IPS), 3-Tier architecture, De-Militarized Zone (DMZ), Network Antivirus/SPAM, Endpoint Security (Antivirus/Malware), SCAP Monitoring Tools that include; Vulnerability, Configuration, Asset and Patch Management

Physical and Environmental Controls include, but are not limited to: Access Controls; Electronic Key Cards, Numbered Key Pad Locks. Fire and Emergency Controls: Emergency Power/Shutoff, Fire Alarms, Smoke Detectors, Emergency Lighting, Lighted Exit Signs, Fire Suppression Systems, Cameras/Electronic Surveillance Systems, Visitor Badges and logs.