US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/06/2016

OPDIV:

AHRQ

Name:

Patient Safety Organization System

PIA Unique Identifier:

P-7192177-095992

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The Patient Safety Rule establishes a framework by which hospitals, doctors, and other health care providers may voluntarily report information to Patient Safety Organizations (PSO), on a privileged and confidential basis, for the aggregation and analysis of patient safety events. The Patient Safety Organization System (PSOS) supports AHRQ's implementation of the Patient Safety Rule by providing a website and a system of components for administering the certification processes for listing of a PSO; verifying that PSOs meet their obligations under the Patient Safety Rule; working with PSOs to correct any deficiencies in their operations; and, if necessary, revoking the listing of a PSO that remains out of compliance with the requirements. The Office for Civil Rights (OCR) administers and enforces the confidentiality protections provided to PSOs.

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

An entity that applies through the PSOS system to begin their PSO certification process must register through the PSOS website. In order to register the primary point of contact must provide a first and last name, organizational email address, organization phone number, organizational mailing address, employment status, and any additional point of contacts that might be associated with the certification process.

Once a user account is created, the PSO will complete a series of online questionnaires to provide data regarding the entities internal operations and procedures as a means of attesting their qualification to become a PSO. AHRQ employees and direct contractors, serving in system administrator and developer roles, provide an AHRQ email and name to be provisioned an account to access the system.

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

Every entity seeking to be a PSO must certify to AHRQ that it has policies and procedures in place to perform the eight patient safety activities specified in the Patient Safety Rule. In addition, an entity must also, upon listing, certify that it will comply with the following seven additional criteria specified in the Patient Safety Rule.

To perform these activities the PSOS will collect, maintain and share: Data regarding the mission and primary activity of the entity are to conduct activities that improve patient safety and the quality of health care delivery of the PSO; Data regarding the appropriately qualified staff (whether directly or through contract), including licensed or certified medical professionals of the applicant PSO; Data validating that the entity is not, and is not a component of, a health insurance issuer; Data from the entity disclosing any financial, reporting, or contractual relationship between the entity and any provider that contracts with the entity; and, Data stating the entity is not managed, controlled, and operated independently from any provider that contracts with the entity.

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

Employment Status

System administrator and developer username and password

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

Employees

Public Citizens

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

PII is collected and used by the PSOS program managers to create a user account for individuals to register organizations as PSOs. With a user account a user may complete their PSO profile that allows AHRQ to determine their eligibility for becoming a PSO. PII provided by AHRQ employees and direct contractors is used to provision an account.

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 913 and 306 of the Public Health Service (PHS) Act (42 U.S.C. § 299b-2 and 242k(b)). Sections 924(c) and 308(d) of the PHS Act (42 U.S.C. 299c-3(c) and 242m(d)) provide authority for protecting restrictions on identifiable information about individuals.

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

Hardcopy

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

0935-0143; 12/31/2017

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.

Individuals can choose not to offer PII to visit the PSOS website. However, in order to start the certification process for an entity to certify through AHRQ as a PSO, users are required to create an account using a name, organization phone number, organization mailing address, and an organizational email address. If a user chooses to provide PII to use the PSOS functionality the information will only be used for the creation of a user account. Individuals are made aware that registration to become PSO requires the collection of PII. Direct contractors who serve as system administrators are notified that their information must be collected prior to being provisioned access to the system. The system owner manages the system account provisioning process.

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.

Users who wish to use the PSOS functionality to certify through AHRQ as a PSO must provide a name, organizational phone number, organization mailing address, and an organizational email address to create a user account. However, users may choose not to provide their PII to create a user account. Users are not provided an option to opt-out of the collection as the process for registering for a user account to gain access to the PSOS system requires the collection of PII. Individuals may contact the PSO Program directly to register as a PSO if they object to using the online form to submit PII data. Direct contractor that service as system administrators must provide their PII in order to be provisioned access to the system.

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

Users and system administrators of the PSOS system will be notified when a change to the system or additional certification processes within the functionality of the system is added that may use PII for a different purpose. Users will be notified through an email notification that is sent to the email used at the time of registration. The notification will detail any changes to the use of PII, or any disclosures of their data as a result of a change to the system or the use of the PII contained within the system. In addition, PSOS provides regular notifications in the forms of system updates to users who sign up for an account.

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.

Users and system administrators who are concerned that PII has been inappropriately obtained, used, or disclosed can contact the PSO Program by sending an email to the AHRQ email found within the Ask a Question of Provide Feedback feature located on http://info.ahrq.gov, or by mail or by phone with information located on the About tab found at https://www.pso.ahrq.gov/about/contact.

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 PSO website system is used only to capture and forward the PII data, along with the other Form data, to the “PSO Database application” – that is external to the system of concern. The checking of the data for integrity, availability, accuracy and relevancy happens outside the PSOS system. PSOs who need to update their registration data may contact the PSO Program.

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

Users:

Have access to their profile to update registration information.

Administrators:

Administrators (direct contractors) have full access to the system to conduct system maintenance activities.

Developers:

Developers (direct contractors) have full access to the system and to the data that resides on the system to troubleshoot user interface issues and to facilitate the use and maintenance of the system.

Contractors:

Direct Contractors, in the role of developers and content editors, work on behalf of AHRQ to ensure system operability and usability.

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

AHRQ employees and direct contractors for this system fill the roles of developers and are granted access to the entire system to manage the user interface and to troubleshoot user interface issues and maintain system operation.

Developers cannot currently be firewalled from the limited PII within the system. Administrator roles are defined and established by the AHRQ PSOS system owner and users are assigned access and privileges by a system administrator under the direction and approval of the PSOS system owner.

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.

Once administrator roles for accessing the PSOS system are assigned and approved by the AHRQ PSOS system owner, a system administrator assigns access based upon the role. Each role within the system is segregated by the ability to access the system, and PII within the system. Roles are managed by the system administrator and any authorized individual who needs additional access to the system, and to the PII that resides on the system, must be approved by the AHRQ PSOS system owner before additional level of access is granted.

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 AHRQ employees and direct contractors that support the system must complete the AHRQ annual Information Technology Security and Privacy Annual Training.

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.

A records schedule is currently pending review and approval at National Archives and Records Administration (NARA). The records schedule addresses the listing and delisting of PSOs and continued certification documentation. Destruction of records is scheduled for five years after delisting.

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

The administrative controls used in this system include the assignment of least privilege. Only administrators that need the necessary access to see information to complete a task have permissions to do so. The technical controls used in this system include systems being configured according to configuration baselines. Systems will be configured according to Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) with possible modifications to ensure that systems have all the necessary functionalities. Physical controls include, but are not limited to the use of locked cabinets to store server hardware, which are housed in an access-controlled, secure data center. All controls are documented fully in the Security Assessment Report (SAR).

Identify the publicly-available URL:

https://www.pso.ahrq.gov/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes