US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/11/2017

OPDIV:

AHRQ

Name:

Patient Safety Organization Privacy Protection Center

PIA Unique Identifier:

P-2407336-860486

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?

Yes

Identify the operator.

Contractor

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.

Change of POC; Increase in number of records to 100-499.

Describe the purpose of the system.

To support the Patient Safety and Quality Improvement Act (PL 109-41), the Patient Safety Organization Privacy Protection Center (PSOPPC) system works with Patient Safety Organizations (PSO) by providing various education services, submission formats and the ability to submit patient safety event information via a web portal. The purpose of the (PSOPPC) system is to facilitate the collection of PSO information to provide research data for the AHRQ Network of Patient Safety Databases (NPSD). PSOs are federally listed organizations that serve as independent, external experts who can collect, analyze, and aggregate Patient Safety Work Product (PSWP) locally, regionally, and nationally to develop insights into the underlying causes of patient safety events. PSWP is data provided voluntarily to the federally-registered PSO by healthcare facilities such as emergency rooms, hospitals, and in-patient and out-patient facilities.

This data generally characterizes an adverse event or incident that occurred to a patient while receiving treatment, near-misses and hazardous conditions. PSOs are established to remove significant barriers that can deter the participation of health care providers in patient safety and quality improvement initiatives, such as fear of legal liability or professional sanctions.

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

There are three types of information that the system collects and maintains.

The system collects organizational information, including a PSO point of contact (POC) first and last name and the PSO POC contact information as a business phone number and business email address, for the purpose of establishing PSO access so that PSWP data may be electronically submitted into the PSOPPC system.

The system also collects information about patient safety events, referred to as PSWP data, that includes patient safety events such as the identification, analysis, prevention, and reduction or elimination of a certain procedure, the risks and hazards associated with the delivery of a specific type of patient care, treatment, and patient treatment results and outcomes. This information is submitted by PSOs voluntarily into the system. The patient event data is first collected by the PSO, submitted to the PSOPPC and rendered non-identifiable before the data is sent on to the NPSD. As a result the system collects information indirectly through the PSO to ensure the confidentiality and privacy of a patient.

The system collects a first and last name, password, and email address from AHRQ employees and direct contractors who are authorized as system administrators and developers, for the purpose of granting access to the system for routine maintenance and system development.

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

The PSOPPC system provides an electronic method for PSOs to report aggregated, non-identifiable data regarding the large number of patient safety events that are needed by AHRQ to understand the underlying causes of patient harm from adverse events and to develop more reliable information on effective strategies for improving patient safety.

To perform this task, PII of PSO POCs is collected by the system, including the name, mailing address, business email, and business phone number, to validate and register a PSO. This information is used to establish access for the PSO to begin submitting PSWP data into the PSOPPC system.

PSWP data represents the largest type and amount of data collected by the system. PSWP data is submitted by PSOs into the system electronically once the PSO account has been established. The initial collection of PSWP data by PSOs may contain birth dates, gender, and ethnicity, however patient names, social security numbers, and medical record numbers are not collected by PSOs. However, PSOs are required to render the PSWP data non-identifiable by removing the name, social security number, medical record number before data is submitted into the system. Submitted PSWP data may contain birth dates, gender, and ethnicity for the purpose of inferring general characteristics about groups of people based on age range, sex, and ethnic background.

AHRQ employees and direct contractors provide an AHRQ email and first and last name as user credentials to be provisioned account access to the system for system development and system maintenance support.

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

Mailing Address

Phone Numbers

Gender

Ethnicity

AHRQ system user information (including username and password)

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Patients

Employees and Vendor/Contractors of Patient Safety Organizations who are system users

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

There are three primary purposes for the use of PII.

PII is collected from PSOs to validate and register the PSO POC to access the system. Access is necessary to submit PSWP data into the system.

PII is collected to provide authorized AHRQ employee and contractor access to the system for routine maintenance and system development.

PII elements, such as date of birth, used to infer age, gender, used to infer sex of patient, and ethnicity are collected by the system so that PSWP data can be analyzed to identify trends within general age ranges, type of sex, and ethnic backgrounds.

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

NA

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.

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

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.

PII that is collected from PSO POCs must be provided for the purpose of establishing access to the system. POCs whose information is collected for this purpose are made aware that this information is required to establish system access.

PSOs serve as the primary collection point for PSWP data. After the collection of this data, the PSWP data is then submitted to the PSOPPC . No PII is required for submission. PSOPPC renders the data non-identifiable prior to submission to the NPSD. No notice is provided to individuals as neither AHRQ nor the PSOPPC knows the identities of any patients. Since this data is collected indirectly, no notice is provided by AHRQ.

PII that is collected from AHRQ employees and contractors is used to establish access to the system for routine maintenance and system development. The contractors are direct contractors to AHRQ who are made aware that this information is required to establish system access.

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.

PSOs who want to be federally-registered by AHRQ data must provide PII to establish access to the system. However, PSOs may choose not to register with AHRQ, thus opt out.

PSWP data is indirectly collected and then submitted voluntarily by PSOs. PII fields are not required for submission. Opt-out options are not directly provided by AHRQ to any individual. Since patient data is collect indirectly, no opt-out is provided by AHRQ.

AHRQ employees and contractors must provide limited PII to establish access to the system to perform system administration and development. The contractors are considered direct contractors to AHRQ and no opt-out is provided to these individuals who must access the system to perform maintenance or development support.

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

PSOs who are federally-registered and have access to the system are notified of any changes to the system regarding the use of the system, or any change in the way PSWP information is submitted into the system. Once notified, PSOs may choose not to participate further based upon the change in system use or data submission.

PSOs serve as the primary collection point for data. After the collection of this data, the PSOPPC renders the data non-identifiable and then submits the data to the NPSD. PSWP data is not maintained as individual records, but as a large data set of anonymized data. As a result, no notice is provided to individuals as a result of a major change 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.

PSO POCs are instructed to contact the PSOPPC Program Help Desk via telephone or by email to address any concerns regarding the use of PSWP data, or PII data used to establish 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.

PSO POC information used to establish access to the system is maintained by system administrators. This information must remain accurate and updated in order for PSOs to continue to maintain their access to the system. In the event of any change of POC information, PSOs are instructed to contact the PSOPPC Program Help Desk to make changes. the PSOPPC program reviews PSO accounts periodically (usually annually) to ensure that the PSO POC continues to meet program requirements to be registered as a PSO.

PSOs serve as the primary collection point for PSWP data. After the collection of this data, the PSO renders the data non-identifiable and then submits the data into the system. PSWP data is not maintained as individual's records, but as a large data set of anonymized data. Data submitted by PSOs is considered accurate and relevant, and there is no process in place to review submitted PSWP data to ensure the integrity, availability, accuracy, and relevancy of this data, as the data is used for statistical and trend analysis only. PSWP data is not maintained as individual's records that require a periodic review.

Direct contractors are required to provide PII, in the form of an AHRQ email and first and last name, to provision system access. Each user profile is reviewed periodically to ensure that the contractor requires access to the system, and to ensure the information is accurate.

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

Administrators:

Administrators access PII of PSO Personnel to provision accounts to manage identity proofing process.

Developers:

Developers, who are direct contractors, have access to PII as part of their responsibilities to develop and maintain system operations.

Contractors:

Direct contractors serve as administrators and developers for the system, and have access to PII as part of these responsibilities.

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

The PSO Program Director and PSOPPC system owner review and authorize all system users based upon the role (system administrator, system developer, or subject matter expert), and review the level of access that the users require to perform their role. Users are assigned a level of access to the system, and role-based permissions built into the system allow the system owner to grant or limit access to PII based upon the assigned role.

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.

Users are assigned a level of access to the system based upon the authorized role that each user will perform. Role-based permissions built into the system allow the system owner to grant or limit access to PII based upon the assigned role. Any change in a role, and subsequent need to know or access PII, must be approved by the system owner. The system owner will grant or limit access based upon the change in the role and the need to know or acess PII.

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.

Annual AHRQ Information Security and Privacy Awareness training.

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

Contractors that support the system functionality and operation conduct additional role based training as part of their organization's training program. This training includes a discussion and requirements of the Patient Safety Act, the Health Information Portability and Accountability Act (HIPAA), and additional federal IT security and privacy requirements. This training is conducted prior to the contractor staff being introduced onto the contract to support the system. The contractors that support the system are direct contractors that are provisioned system access to provide system development and maintenance support.

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.

Destruction of electronic information, at the end of the contract or as appropriate, via sanitization of the systems holding the information. Locked shred bins are utilized for document and media destruction and certificates of destruction are received from the bonded destruction company upon completion.

The National Archives and Records Administration (NARA) retention schedule for PSO-PPC can be found under Record Control Schedule N1-510-09-001.

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

Technical controls include but are not limited to: authorized users using user passwords and a hard token-One Time Password Device for access to the secured areas of the website, separation of duties, filters and parameters are set up in accordance with an approved configuration to enforce the security policy, data back up on a daily and weekly basis, with the weekly tapes going off-site for storage, destruction of electronic information, as appropriate, via sanitization of the systems holding the information, audit of events initiated by each individual user, i.e., entry of UserID and password, program initiation, file creation, file deletion, file open, file close, and other user related actions, audit trails identify the individual user initiating the event, date, and time the event occurred, success, or failure of each event, and location where the event was initiated.

Physical controls include but are not limited to: building access cards and ID badges are required in the main facility and only authorized personnel have access to the locked data center where the hardware used to process this system data is located, security guards are present during working hours and off-hour visits are made by security personnel, CCTV is used for monitoring of the facility, back up media is stored offsite in a secure, climate controlled storage facility, visitor process includes signing in and out, visitor badges and escorting of all visitors, uninterruptible Power System (UPS) with a diesel generator back up to ensure ongoing system operation and an orderly shutdown when necessary.

Power to the data center is separated from the power to the rest of the facility and additional HVAC with humidity controls is in place. Locked shred bins are utilized for document and media destruction and certificates of destruction are received from the bonded destruction company upon completion.

Administrative Controls include: procedural safeguards: Users must comply with terms of use on reinforce the confidentiality protection requirements, and the confidentiality policy is reviewed and signed on an annual basis, security training and ongoing awareness programs, such as posters and newsletters.
Access controls include: termination procedures to ensure only authorized personnel have access to facilities and systems, commensurate with their job duties, review of system activity logs to monitor for issues, Risk Management plans to include Risk assessments, Security Plans, Continuity of Operations/Disaster Recovery plans, background and reference checks are performed on all IFMC personnel.

Identify the publicly-available URL:

www.psoppc.org

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.

Does the website have any information or pages directed at children uner 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