US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/29/2022

OPDIV:

AHRQ

Name:

PSOPPC Opioid Collaboration System (OCS)

PIA Unique Identifier:

P-7647337-102957

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?

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.

No Changes Have Occurred.

Describe the purpose of the system.

The Opioid Collaboration System (OCS) is a child system of the Patient Safety Organization Privacy Protection Center (PSOPPC) system. The PSOPPC system enables Patient Safety Organizations (PSO)s to submit Patient Safety information to the PPC. The OCS is only accessible via the PSOPPC to registered users of the PSOPPC. Registered users are PSOs, the PSO are qualified workforce members, including licensed or certified medical professionals

The OCS provides collaboration functionality to members of the PSOPPC system. AHRQ is providing this system for PSOs to voluntarily collaborate on approaches to addressing the

Opioid crisis and to improve healthcare practices. This bulletin board-like system will provide users the ability to post comments, polls, use calendars, upload files and share information with other members of the system.

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

OCS users are required to be members of the PSOPPC system. User identity information (name, organization, email, phone, mailing address, user name and password) is collected and maintained within the PSOPPC system boundary.

Usernames and passwords are validated by the PSOPPC to grant access to OCS. OCS uses user names, organization and email address.

The system will collect discussion threads, documents, presentations, calendar appointments.

The system will display the name of the person posting information (comments, polls, files, appointments). The OCS will email summary digests to OCS members.

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

The OCS uses Software as a Service (SaaS) Salesforce Community functionality to enable users to share ideas and information by posting comments, polls and uploading files related to the Opioid crisis to the system.

Users access the OCS after logging into the psoppc.org site and after reviewing and agreeing to Terms Of Use (TOU).

Once on the OCS, users can read and add content (files, comments, polls, join/leave groups) and edit their own content.

The system administrators will monitor OCS by reviewing content for inappropriate content (including PII). The user added content may include personally identifiable information (PII), however, system administrators will monitor for and remove that PII. System administrators will maintain the system, including granting and revoking access to the system.

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

Yes

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

Username and Password

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

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

OCS displays users name to indicate who posted a comment, uploaded a file or is sharing information. Email is used to notify users of activity (posts, uploads etc.) on the OCS.

The PSOPPC system uses PII is used to verify the user's identity and create a username and password.

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. Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Information Collection has been approved for the Patient Safety Organization systems for which PSOPPC OCS is a component:

OMB Collection Approval Number: 0935-0143
Expiration Date: 9/30/2024

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.

Registered Patient Safety Organizations must have a PSO Agreement on file before their personnel may register for an account on the PSOPPC Website and before they can access the OCS. These documents contain language which advises how PII will be used. Individuals voluntarily submit personal information while applying for user IDs to the PSOPPC system.

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.

Registered Patient Safety Organizations must have a PSO Agreement on file before their personnel may register for an account on the PSOPPC Website and be granted access to the OCS. These documents contain language which advises how PII will be used. Should the need arise to change the usage or sharing of PII, the PSO Agreement will be updated and new agreements will be delivered to affected parties. Individuals are given written notice.

There is no requirement for a user to gain access to this system outside of their voluntary desire to become a PSO and participate in the community activities. Any user who does not agree to the information in an identifiable form (IIF) usage practices may choose not to become a system user.

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 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.

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 are instructed to contact the PSOPPC Program Help Desk via telephone or by email to address any concerns regarding the use of 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 user 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 user 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 users continues to meet program requirements to be registered as a PSO.

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.

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 access 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.

All users must agree to a Terms of Use (TOU) agreement before being granted access to the system. Additionally, a disclaimer is presented to the end user before they can get access to the system.

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

ActioNet (contractor) personnel complete Annual AHRQ Information 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.

Administrative, technical and physical controls as specified in the Salesforce FedRAMP authorizations.

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, including 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 personnel.

Identify the publicly-available URL:

Access to the OCS is only available to users of the PSOPPC website and only accessible via the PSOPPC website (https://www.psoppc.org).
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.

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?

No

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

null