US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/16/2022

OPDIV:

AHRQ

Name:

AHRQ AWS Enclave

PIA Unique Identifier:

P-7991713-180794

The subject of this PIA is which of the following?

General Support System (GSS)

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?

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.

N/A

Describe the purpose of the system.

Shared Infrastructure is a General Support System (GSS) composed of servers, firewalls, workstations,
operating system software, data, and network infrastructure components. The GSS supports all of the systems within the Amazon Web Services (AWS) Enclave; AHRQ.gov, the Children's Health Insurance Program Reauthorization Act (CHIPRA), Digital Media, Effective Healthcare Act system (EHC), Health Literacy application, Patient Safety Organization system (PSOS), Quality Indicators system, Systematic Review Data Repository (SRDR), USPSTF.gov, Shared Infrastructure, and ATLAS.

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

Information is collected from AHRQ employees, including employment status, mailing address, and phone number, as a means of establishing account access to the system. The system supports web interfaces and applications servers that allow these users to communicate internally at AHRQ.
Information is collected from members of the public who wish to ask a question regarding a particular AHRQ program or submit feedback. This information includes PII (personal identifiable information) that contains a name and email address.
PII collected from direct contractors who serve as users/system administrators in order to access the system, consists of user credentials (i.e. username, password, Personal Identity Verification (PIV) card and/or email address). Users/system administrators include AHRQ employees and direct contractors (using HHS user credentials only).

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

PII is collected from members of the public to allow feedback and for members of the public to ask questions related to an AHRQ program. This PII is used to respond to an inquiry or feedback as applicable.
PII collected from AHRQ employees and direct contractors, in the form of name, email address, phone number, employment status, and mailing address, user credentials (i.e. username, password, Personal Identity Verification (PIV) card and/or email address). is collected on a voluntary basis to enable communication. Administration of system modules takes place via web interfaces on internal application servers accessible only from the internal AHRQ network.

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

Yes

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

PIV card

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?

The application collects a very limited amount of PII to respond to requests from a user of the website (for example, to respond to public feedback or questions), to provide email updates to members of the public who choose to provide their email address to receive program updates. Direct contractor user credentials are collected to provision system access for development and administrative purposes.

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.

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.

Users are notified of potential uses of PII AHRQ's privacy policy which states the following: Users are not required to provide personal information to visit any of our Web resources; If users choose to provide AHRQ with additional information about themselves through an E-mail message, form, survey, etc., AHRQ only uses that information to respond to their message or to fulfill the stated purpose of the communication. The information provided is handled on a confidential basis within the Agency. System administrators are required to provide their PII to establish system access, and notification of this collection is made during the process to establish this 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.

Users and system administrators are able to opt-out of the collection of their PII by sending an e-mail to info@ahrq.gov stating that they object to the information collection or use of their PII.

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

Members of the public who elect to provide an email address to receive program news and updates will be alerted via email for any changes in the use of their email. System administrators are required to provide their PII to establish system access. This information is required and users are made aware of the need prior to the collection to grant access.

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.

Members of the public may contact the program by mail, phone or electronic message submission through the AHRQ website to address a concern. System administrators must provide PII to establish system access. System administrators may contact the system owner directly with any concerns that arise from system administrators regarding the use of their PII.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Members of the public who wish to update their email address may contact the AHRQ program by mail, phone or electronic message submission through the AHRQ website to address a concern. Information collected from members of the public is not used in any manner to make determinations of benefits or decisions about the individual. As a result, there are not system processes in place to ensure the integrity, availability, and relevancy of information about individuals. Information is used only to respond to an individual’s feedback or question.

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.

Roles are defined and established by the AHRQ business owner point of contact and users are assigned access and privileges by a system administrator under the direction and approval of the business 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.

Permissions are limited through the use of system roles that were identified during the requirements gathering phase of the project. The system roles only allow access to a minimum amount of information necessary for system administrators to adequately perform their job.

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 AHRQ GSS 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.

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 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).