

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

02/06/2024

**OPDIV:**

AHRQ

**Name:**

Portal System

**PIA Unique Identifier:**

P-2742418-553672

**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.**

PIA updated to better reflect current system components and functionality, information collected.

**Describe the purpose of the system.**

the National Resource Center (NRC) Portal supports a consolidation of websites and web applications to collect information regarding the current state of health information technology:

The system supports a consolidation of websites and web applications to collect information regarding the current state of health information technology, including: <https://digital.ahrq.gov/>; <https://cds.ahrq.gov/>; The system supports the collection and communication of information in the form of national reports, AHRQ funded projects, digital healthcare tools and resources, key topics, and funding opportunities, knowledge and findings that everyday clinical practice;; web resources for the Government's efforts to integrate information technology throughout all areas of healthcare; blogs to answer questions about the nation's transition to electronic health records, and to create a

conversation about the challenges and successes health care providers, physicians, practices, and organizations are experiencing as they transition from paper to electronic health records;

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

The NRC portal also has a group of contractors (fewer than 20 at any time) who log onto the respective sites to update content, perform system updates to the Drupal core and custom applications, and perform other system-related tasks. The system collects the following data for System Administrators, System Developers, and Content Contributors users of this system: User Name, Email Address, Password, User Status (Active / Blocked), Role (Authenticated User, Administrator, Content Manager), and Locale / Time Zone.

The NRC Portal also has a variety of mechanisms for any public user to provide feedback or request support. These forms are completely optional, and collect a minimal amount of data, including the person's name, email address, and through log files, an IP address.

The NRC portal also has 5 users who log onto the site to update content, perform system updates to the Drupal core, and perform other system-related tasks. The system collects the following data for System Administrators, System Developers, and Content Contributors users of this system; User Name, Email Address, Password, User Status (Active / Blocked), Role (Authenticated User, Administrator, Content Manager), and Locale / Time Zone.

The NRC Site also has a Contact Us form for any public user of the site to provide feedback (<http://healthit.ahrq.gov/contact-us>). This form collects the person's name and email address, by the Web site user when users submit feedback.

In some cases, other information such as documents, files, and links may be posted or shared, but these documents are not expected to contain any PII and the submission is entirely voluntary. One site allows users to post pictures of themselves, but again that is optional and intended to be shared publicly by the users doing the posting.

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

The system collects (Personal Identifiable Information) PII from System administrators and system developers (name & email address) to provision AHRQ account access to the system to perform regular system development and maintenance for system functionality.

Information collected from research projects that are funded by AHRQ is shared publicly and is consolidated and maintained in a searchable format within the web application for review and research. Public users have the ability to provide PII that is used by the system to send AHRQ Health Information Technology E-Mail updates about the AHRQ Health Information Technology Portfolio Program. Users may also submit PII to provide feedback through a Contact Us form. PII collected for email updates and for feedback is only for these purposes and is not shared for any other intended use.

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

Yes

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

Name

Photographic Identifiers

E-Mail Address

Phone Numbers

User credentials, time zone, (locale), IP address and Web browser  
User Status (Active / Blocked)  
Role (Authenticated User, Administrator, Content Manager)

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

Employees  
Public Citizens  
Business Partner/Contacts (Federal/state/local agencies)

**How many individuals' PII is in the system?**

500-4,999

**For what primary purpose is the PII used?**

PII is collected and used in four primary ways; 1) PII is collected through either a Contact Us form, or through an established email for public users to collect feedback or to ask a question about data, program updates, or to report an issue with overall system performance and navigation; 2) PII is collected to provision and maintain user accounts. User accounts provide access to additional information within the system, and also allows the user to customize the user interface based upon the types of information they would like to review; 3) PII is collected from system administrators for the purpose of developing and maintaining the system and the various websites and applications that are supported within the system; 4) PII is provided by the users themselves for public consumption, such as posting a blog or submitting a photograph of themselves to be displayed in collaborative forums.

Unless explicitly stated, PII collected by the system is not shared in any way nor disclosed to any person or entity outside of the system.

**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?**

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.**

**Identify the sources of PII in the system.**

Directly from an individual about whom the information pertains  
Email  
Online

**Identify the OMB information collection approval number and expiration date**

Not Applicable - By statute, the Paperwork Reduction Act (PRA) does not apply to some types of information collection. OMB approval is not required for information collection that is submitted in response to general solicitations of comments from the public, regardless of the subject. In addition, the information collected by the system is administrative in nature, for example, the use of user accounts to complete development or maintenance activities for the system.

**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 that wish to provide feedback or to ask a question may use either the Contact Us form or the email that is provided for the purpose of collecting such information. In both cases users are notified that the electronic form, or the provided email, informed that contact information may be shared with content managers. In this case, content managers are AHRQ employees that support the programs, and the system web applications and websites provide information that support these programs. The notice is to inform users that PII might be shared with the AHRQ programs to help with answering an inquiry or to address feedback. PII submitted by any user may be deleted upon request.

**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 provide feedback or a question volunteer their PII, in the form of a name an email address, and/or a phone number, to provide this information. If users do not wish to provide PII, they may also call AHRQ directly and be transferred to the program in question to ask a question or provide feedback.

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

Submission of this information is voluntary, is only disseminated to AHRQ program employees or system administrators to ask a question or to provide feedback. There are no anticipated major changes for the use of PII data in the information system, so there is no process to obtain consent for this. However, if the system develops additional capabilities that involves PII for additional navigation of the system, or additional features that require user accounts to be upgraded, system administrators will notify users of the change to the way PII will be used, and during notification users will be able to delete their accounts or access the changes to the use of PII within 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.**

Users who have concerns that their information has been inappropriately used can contact the system administrators via phone, email, or online form. The system administrators will either disable/delete the user account, or work with users to change passwords to prevent the compromised account from causing any further damage or harm.

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

All PII collected and maintained within the system is from user sources, including information used to provision user accounts and to provide feedback of ask a question. User information is not used for any other purpose, and there are no evaluations or determinations made about an individual based upon the PII. As a result, there is no periodic review of PII contained within the system. Should users need to change information about themselves, such as an updated email address or name, users can contact the system administrators to request this change.

**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.**

System accounts are limited system administrators who are responsible for managing accounts for their website or web application supported by the system. The system owner is responsible for approving account creation requests and notifies system administrators to create accounts. Should an individual user request that an account be deleted, the System Owner will send a request to the system administrators to delete the account in questions. The system owner limits all system administrator account creation and monitors the number of users who have access to the system, and to PII, at all times as part of the system owner 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.**

The System Owner's approval for all new privileged account is based on the access needed for a user to perform his/her duties and is contingent upon that user's favorable adjudication of AHRQ security/background investigations. System administrators review system accounts on an annual basis to ensure that system accounts present on the system and their associated access privileges are consistent with those initially authorized and to ensure that accounts associated with users no longer requiring access have been disabled or terminated. Shared accounts are not permitted. Additional Access Controls as required by NIST SP800-53 Rev 4 are outlined in the System Security Plan.

**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.**

System personnel take the AHRQ security awareness training on an annual basis. New users are provided with training within 30 days of onboarding onto the system support team. Additionally, security awareness training is provided when required by changes to the system.

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

All direct contractors review and sign the role-based security training provided by HHS.

**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.**

When a portal account is deleted, no record of the users' PII (email, phone number, etc.) is retained within the portal. Specific to data collection, the Portal system follows National Archives and Records Administration (NARA) NI-510-09-10. Records maintained in the system are considered temporary - cut off is considered to be the end of the calendar year in which the resource is determined to be superseded or obsolete by the National Resource Center (NRC). Records are deleted or destroyed 6 months after cutoff or whenever no longer needed for business purposes, whichever is later.

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

Technical controls, such as Secure Socket Layer (SSL) software and technology, have been implemented to protect private information (such as login credentials) in transit. Administrative controls, such as password complexity rules have been implemented and password controls have been configured to lock out accounts with too many invalid login attempts. The system comprises development and production environments hosted at a Federal Risk and Authorization Management Program (FedRAMP) certified cloud service providers (CSPs): Acquia Cloud. There are no physical

facilities within the authorization boundary of the system. Additional administrative, technical, and physical security controls required for the system are defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. All controls have been evaluated as part of the system.

**Identify the publicly-available URL:**

The NRC Portal is comprised of a variety of web sites collectively referred to as the "NRC Portal":

CDS Connect (<https://cds.ahrq.gov/>)

NRC (<https://digital.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.**

**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