US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/06/2016

OPDIV:

AHRQ

Name:

Portal System

PIA Unique Identifier:

P-8762597-771274

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?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The following types of information are contained within each of the web applications that make up the NRC Portal; https://healthit.ahrq.gov/; https://pbrn.ahrq.gov/; http://healthit.gov; http://healthit.gov/buzz-blog/; http://pcmh.ahrq.gov/; http://integrationacademy.ahrq.gov/; https://ecqi.healthit.gov/; http://dashboard.healthit.gov/; https://bonnie.healthit.gov; http://ushik.ahrq.gov/; http://cypress.healthit.gov/.

Additionally, the NRC Portal team manages the following administrative applications for the system administration for the purposes of documentation (wiki), ticketing (support), and automated software builds (bamboo); https://ahrqadmin.org/wiki/; https://ahrqadmin.org/support/; https://ahrqadmin.org/bamboo/.

healhit.ahrq.gov: This web application was created as a consolidation of information regarding the current state of health information technology. It provides information in the form of national reports, AHRQ funded projects, health IT tools and resources, key topics, and funding opportunities, and knowledge and findings that everyday clinical practice.

https://pbrn.ahrq.gov/: This web application is provided as a public resource center for information regarding primary care practice-based research networks (PBRN). PBRNs are a group of ambulatory practices devoted principally to the primary care of patients, and affiliated in their mission to investigate questions related to community-based practice and to improve the quality of primary care.

http://healthit.gov/: This website serves as the homepage for the Office of the National Coordinator (ONC) for Health Information Technology. It is a centralized, consolidated resource for the Department of Health and Human Services (HHS) to provide a comprehensive web resource for the Government's efforts to integration information technology throughout all areas of healthcare.

http://healthit.gov/buzz-blog/: This application is a web service of HHS ONC. It is a blog created 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.

http://pcmh.ahrq.gov/: This website is the homepage and resource center for he patient centered medical home (PCMH), a model created by AHRQ for transforming the organization and delivery of primary care.

http://integrationacademy.ahrq.gov/: This website is referred to as The Academy is provided for public consumption. The website functions as both a coordinating center and a national resource for people committed to delivering comprehensive, integrated healthcare.

https://ecqi.healthit.gov/: This website functions as a collaboration center for current resources to support Electronic Clinical Quality Improvement, referred to as eCQI. It provides resources for the purpose of allowing professionals who are dedicated to clinical quality improvement for better health.
http://dashboard.healthit.gov/: This website is an interactive Health IT dashboard maintained by ONC. The dashboard provides access to analysis, research, public datasets, and more on health IT and ONC programs for public consumption.

https://bonnie.healthit.gov/: Once a CQM has been loaded into the Bonnie application by a user, the user can inspect the measure logic and then build mock test records and set expectations on how those test records will calculate against a measure. The resulting information provides results on whether the eCQM is able to accurately measure mock data to provide a desired EHR.

http://ushik.ahrq.gov/: The United States Health Information Knowledgebase (USHIK) is an on-line, publicly accessible registry and repository of healthcare-related metadata, specifications, and standards.

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

The NRC portal also has 10 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 by the Web site user when users submit feedback.

The Splunk log correlation tool, which is used to analyze web site traffic patterns and troubleshoot problems experienced on this and other web sites, collects partial PII. Specifically, three fields are collected: User Agent (i.e. browser), User Name (if applicable), and IP Address. The Web site also has Google Analytics, which collects information about user browers, location, IP.

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

The system collects PII from System administrators and system developers to provision AHRQ account access to the system to perform regular system development and maintenance for system functionality.

Information collected from ONC programs and research projects that are funded by ONC 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.

Individual blog authors who wish to discuss an issue or challenge within health IT provide their content for publication on the ONC Buzz Blog. The information is broken into subsections for public consumption and includes blogs on electronic health and medical record implementation, meaningful use standard updates, EHR case studies, and privacy and security of EHRs. Individual authors are profiled on the blog they write with a picture. The Blog also allows users to reply to an individual blogpost by providing their name, email, and website url if applicable. In addition, users may provide their email to receive alerts when a new blog post is published. PII, such as the name of the person replying to the blog, is provided publicly along with their comment, but the email address collected during a Blog rely is not shared and only used when a the individual requests that the reply be removed from the Blog.

The types of information shared for public consumption through application provides new research findings submitted by the behavioral health and primary care research field (both federal and private organizations), information about specific federal initiatives, and events and activities focused on the integration of behavioral health industry. No PII is collected, shared, or maintained through this web application.

https://ecqi.healthit.gov/ is a collaboration with ONC and CMS for public consumption, and research, latest news, and upcoming events are sourced from these agencies for consolidation within the website. Public users can ask a question or provide feedback by emailing the eCQI general email, however there is no electronic form for any type of collection, other than an email address that users would use to email a question.

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

Phone Numbers

User credentials

Time Zone

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 three primary ways; 1) PII is collected through either a Contact Us form, or through an establish 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.

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?

No

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable - By statute, the PRA does not apply to some types of information collections. OMB approval is not required for information collections that are 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 within the system functionality.

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. For the ONC Bluz Blog, users that have provided a reply to a specific Blog may email to have their response removed from the blog they replied to.

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 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 and to provide feedback. For the ONC Bluz Blog, users may reply to a blog for discussion by providing a name and email. Users that do not provide this information cannot provide a reply.

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, collection of disclosed can contact the system administrators. The system administrators will either disable 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.

Administrators:

To maintain user accounts on the system and to direct feedback or questions to the appropriate AHRQ program point of contact.

Contractors:

To maintain user accounts on the system and to direct feedback or questions to the appropriate AHRQ program point of contact.

Others:

Users who have direct access to their account details for account management.

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 resources is 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 two FedRAMP certified cloud service providers (CSPs): Amazon Web Services (AWS) and 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:

https://healthit.ahrq.gov/

https://pbrn.ahrq.gov/

http://healthit.gov/

http://healthit.gov/buzz-blog/

http://pcmh.ahrq.gov/

http://integrationacademy.ahrq.gov/

https://ecqi.healthit.gov/

http://dashboard.healthit.gov/

https://bonnie.healthit.gov/

http://ushik.ahrq.gov/

http://cypress.healthit.gov/

https://ahrqadmin.org/wiki/

https://ahrqadmin.org/support/

https://ahrqadmin.org/bamboo/

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.

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