US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/23/2016

OPDIV:

AHRQ

Name:

Systematic Review Data Repository (SRDR)

PIA Unique Identifier:

P-2781345-698669

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

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.

In an effort to reduce the burden of conducting systematic reviews of data such as medical evidence maps, reviews of diagnostic test performance data, technology assessment data, and technical brief data, researchers and developers at the Brown University Evidence-based Practice Center (EPC) (previously at Tufts Medical Center), with support from the Agency for Healthcare Research and Quality (AHRQ), developed a collaborative, Web-based repository of systematic review data. These reviews refer to a comprehensive assessment of healthcare literature and collected healthcare reports. This allows the research community to build upon previous research as opposed to duplicating efforts.

The Systematic Review Data Repository (SRDR) primarily facilitates the data extraction and storage of these types of data to start new systematic review projects, create extraction formats of data for review, and to extract and store data for analysis. This database application is provided to members of the public as a resource and is freely accessible to facilitate evidence reviews and thus improve and speed up policy-making with regards to healthcare.

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

The SRDR is capable of supporting systematic reviews of data such as medical evidence maps, reviews of diagnostic test performance data, technology assessment data, and technical brief data. The system primarily facilitates the data extraction and storage of these types of data to start new systematic review projects, create extraction formats of data for review, and to extract and store data for analysis. Members of the public may provide personal information in order to create a user account to interact with the database, to include name, email address, and password. Members of the SRDR Team including AHRQ employees and individuals from Brown University, provide a name and organization contact information as a point of contact and to identify the SRDR Program Board of Directors on the website. The system also collects user credentials, to include name, AHRQ email, and password, to provision account access for direct contractors to perform system administration and development.

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

The SRDR supports systematic reviews of the following medical community registries: the Complementary and Alternative Medicine Bibliography, the Oregon Health and Science University (OSHU) Method Bibliography, and the SRDR Public Primary Publications. Data that exists within the registries that the SRDR searches does not contain personally identifiable information (PII). The system primarily facilitates the data extraction and storage of these types of data to start new systematic review projects, create extraction formats of data for review, and to extract and store data for analysis.

Users may create a user account to search a specific registry to search data using title, abstract, PubMed ID, Author, Year, or Journal to find targeted data. The system collects first name, last name, organization name, and organizational email address to provision an account to provide the ability of users to leave comments or pose questions for systematic review projects. Users may create a systematic review of projects, be a project contributor, a public commentator, and publish systematic data reviews by creating a SRDR account. The system also collects system administrator and system developer data, such as name, AHRQ email and password, for the purpose of provisioning account access to AHRQ employees and direct contractors. AHRQ employees and members of the SRDR Board of Directors provide a name and organizational information to facilitate questions or inquiries about the program.

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

System administrator and developer username and password

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

Employees

Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is collected from members of the public to create a user account. With a user account a user may create a new project; add, edit and delete extractions of published data from data registries; provide comments to an existing project, and close and delete research projects. PII is also collected from the SRDR Board of Directors to serve as a point of contact for the program. PII is also collected from AHRQ employees and contractors to provision access to the system.

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

There are no secondary uses of PII.

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

Other

Identify the OMB information collection approval number and expiration date

0935-0231; 5/31/2019

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 and system administrators are notified at the time of registration that PII is collected to create a user account to access system modules. Users must then submit PII in order to create and account and access these modules.

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 use the SRDR functionality to conduct systematic data review projects must provide a name, an email address, and a password to create a user account. However, users may choose not to provide their PII. Users are not provided an option to opt-out of the collection, as the process for registering for a user account to gain access to the systematic data review functionality allows individuals to choose to use the functionality.

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

Users of the SRDR system will be notified when a change to the system or additional systematic data review functionality of the system is added in later versions. Users will be notified through an email notification that is sent to the account used at the time of registration. The notification will detail any changes to the use of their data, or any disclosures of their data as a result of a change to the system or the use of the PII contained within the system. In addition, SRDR provides regular notifications in the forms of emailed system updates to users who sign up for an account.

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 are concerned that PII has been inappropriately obtained, used, or disclosed can contact the SRDR by sending an email to the AHRQ email, or by mail or by phone with information located on the Contact Us tab found on http://srdr.ahrq.gov/.

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

Users who access the system must provide a username and password to access the SRDR systematic data review functionality of the system. Once logged in users have the ability to manage their user information to ensure that their information is up to date and accurate. If any PII that is part of the account information is incorrect, individuals will experience issues logging into their account. SRDR does not review user account information to ensure the accuracy, relevancy, integrity, or availability.

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

Users:

Users will have access to their individual PII for use logging into their account and to update any information about themselves.

Administrators:

Administrators have read only access to the user profiles in order to perform system administration duties and to maintain system and website functionality.

Developers:

Developers have full access to the system and to PII to troubleshoot system issues or to support user account maintenance and issues.

Contractors:

Direct contractors act as administrators and developers for system maintenance.

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

Direct contractors for this system fill the roles of developers and administrators and developers. Both of these roles are granted access to the system by the system owner, who reviews and manages the provisioning of user account access. Roles are defined and established by the SRDR business owner and system owner before roles are assigned and access is provisioned to ensure that roles that require access to PII are clearly established and managed.

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.

Once roles for accessing the SRDR system are assigned and approved by the AHRQ SRDR system owner, system administrators and developers must be provisioned user credentials and use a personal identity verification (PIV) card to log into SRDR to use the system. These roles are also granted a username and password to access the system as well.

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 SRDR system must complete the AHRQ Information Security and Privacy training annually. Employees and contractors must also review and acknowledge the AHRQ Roles and Responsibilities prior to the provisioning of an account for the access to the system.

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 require users to always have a password to access a user account. The technical controls used in this system include a system wide deployment of Trend Micro Deep Security and Tenable Nessus scanner to detect and mitigate malicious code. 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).

Identify the publicly-available URL:

http://srdr.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.

Session Cookies that do not collect PII.

Persistent 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?

No

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

null