US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/26/2017

OPDIV:

AHRQ

Name:

U.S. Preventive Services Task Force (USPSTF)

PIA Unique Identifier:
P-4806347-587211

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

Does the system include a Website or online application available to and for the use of the general public?
No

Identify the operator.

Agency

Is this a new or existing system?
New

Does the system have Security Authorization (SA)?
No

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

Describe the purpose of the system.

The USPSTF Extranet system was created to provide a collaboration environment for the activities of the U.S. Preventive Services Task Force (USPSTF), an independent, volunteer panel of national experts in prevention and evidence-based medicine. The Task Force works to improve the health of all Americans by making evidence-based recommendations about clinical preventive services such as screenings, counseling services, and preventive medications.

Task Force members come from the fields of preventive medicine and primary care, including internal medicine, family medicine, pediatrics, behavioral health, obstetrics and gynecology, and nursing. The Agency for Healthcare Research and Quality (AHRQ) has been authorized by Congress to convene the Task Force and to provide ongoing scientific, administrative, and dissemination support to the Task Force.

The USPSTF Extranet system is located within the FedRAMP Box Software as a Service (SaaS) environment.

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

The USPSTF Extranet system will collect name and email address for the purpose of account creation. Once an account is created, users may share a variety of information related to preventative services. It is unknown if the documents shared by users may include PII.

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

The USPSTF Extranet system hosts research and recommendation content on real-time feedback from USPSTF board members as a means of transparency for the USPSTF program. Once selected, member duties include prioritizing topics, designing research plans, reviewing and commenting on systematic evidence reviews, discussing and making recommendations on preventive services, reviewing stakeholder comments, drafting final recommendation documents, and participating in workgroups on specific topics and methods. The PII collected is strictly for the purpose of credentialing users.

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

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

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

This system requires the email address to create an account to access the environment. The administrator of this system provides the login details to the authorized AHRQ staff. The UserIDs are created based on the user's email ID. PII is also used to provision accounts for system administrators and developers.

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.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable.

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 that their personal information will be collected at the time in which their account is created. AHRQ employees and direct contractors provide information for the purpose of creating accounts for their roles. Employees and direct contractors are informed that they must provide PII in order to be provisioned an account.

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.

Individuals may opt-out of the collection or use of their PII by contacting AHRQ and stating the corrective action sought and the reason(s) for requesting the correction or elimination of their PII. All other individuals may request to opt-out by accessing their user profile.

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

Users who provide PII will be alerted to any change in the use of their information, and can choose not to have their information used for a new purpose. Direct contactors, performing as developers and administrators, are aware of system changes. Therefore, no notification is given to this group of individuals.

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.

USPSTF Extranet users who believe their PII has been used or shared inappropriately may contact the administrators to address a concern. If a concern is received regarding the use of inappropriate collection of PII, the USPSTF Extranet administrators will review the concern and take appropriate action. Direct contractors provide system administration and developer support and can directly discuss any issue with the misuse of their information with the system owner.

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

USPSTF Extranet users may directly provide updates to their PII in the event of a change of contact information or a change in the place of employment. There is no formal process in place to conduct periodic reviews of PII to determine the integrity, accuracy, availability, and relevancy.

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

Users:

USPSTF Extranet users may update their own data upon login.

Administrators:

Administrators may access PII in order to communicate with users.

Developers:

Developers have access to the system to provide system maintenance, ensure system operations, and maintain the system.

Contractors:

Direct contractors may serve as administrators and developers on behalf of AHRQ.

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

System user access to the data is permitted only through authorization by the AHRQ Project Director, after completion of the required data use agreements, security and privacy awareness training, public trust background check, and database-specific security training. For this system, only authorized administrators will have access to the PII for account management.

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 USPSTF Extranet system are assigned and approved by the AHRQ USPSTF system owner, a system administrator assigns access based upon the role. Each role within the system is provisioned access to the system, and PII within the system. The system administrator manages roles and any authorized individual who needs additional access to the system, and to the PII that resides on the system, must be approved by the AHRQ USPSTF Extra system owner before additional level of access is granted. AHRQ employees and director contractors must use a personal identity verification (PIV) card to access the AHRQ network and a provisioned a username and password to access the USPSTF EXT system.

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 USPSTF Extranet system must complete the AHRQ annual Information Technology Security and Privacy All AHRQ employees and direct contractors must complete AHRQ Information Security and Privacy Awareness Training before accessing AHRQ systems.

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.

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.

The technical controls used in this system include processes in place to create a spam free environment by using the Simple Mail Transfer Protocol (SMTP) server. The SMTP server requires authentication to send email.

All controls are documented fully in the Security Assessment Report (SAR).