US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/17/2017

OPDIV:

SAMHSA

Name:

SAMHSA Knowledge Network

PIA Unique Identifier:
P-5516981-970775

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?
Yes

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.
The Substance Abuse and Mental Health Services (SAMHSA) Website EXTRANET provides information delivery services to the substance abuse and mental health practitioners and professionals on a 24 hours a day, seven days a week. It will serve as a consolidation of the various technical assistance, collaboration and training platforms across all of the different SAMHSA Centers and Offices including anyone who registers for access. The SAMHSA Knowledge Network provides a platform to enable SAMHSA to become a Center of Excellence and a recognized leader in the provision of behavioral health training, technical assistance (TA), and collaboration tools across the nation's behavioral health workforce. It will house all training materials, discussion boards, technical assistance etc. in order to provide a one-stop shop for users.
SAMHSA uses the GovCloud region of Amazon Web Services (AWS) which was created specifically to support the special security needs of the Federal government. GovCloud facilities are staffed by and accessible to US-based persons and are for federal government customers only.

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

Data collected: Information collected from users/system administrators in order to access the system, consists of user credentials (i.e. email address/username, password and google authenticator). Users/system administrators include SAMHSA employees and direct contractors (using HHS user credentials only). Those individuals outside of SAMHSA employees and direct contractors supply users name / email address and password. Potential other fields could be Organization's name, address (business), and business phone number. Other than SAMHSA grantees, related business organizations, practitioners, and professionals, individuals or their organization who register with a name and email address may have limited access. The system publishes metadata regarding Tools, Resources and Courses that may be available either on the system itself or available on other external systems. It also provides a forum capability for users to collaborate and have discussions. The basic system is available to anyone who wishes to create a login and provide the stated information (name, email, business address, business phone, etc). No other information is collected from Other HHS OpDiv. This is the only PII that is requested in the system.

General users of the system may be SAMHSA or non SAMHSA such as general public. Administrative users will only be SAMHSA personnel.

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

The SAMHSA Knowledge Network provides a platform to enable SAMHSA to become a Center of Excellence and a recognized leader in the provision of behavioral health training, technical assistance (TA), and collaboration tools across the nation's behavioral health workforce. Through an extensive content inventory process, existing training and technical assistance content will be categorized, defined, described, tagged, and presented in a unified location for easy access.

Please note that public facing resources will be available to all visitors, grantees and SAMHSA staff will have access to additional training and technical assistance resources delivered to grantees. While there is a targeted cross-section of the public, it is not restricted by the system to create a login. When the system goes live, public users must use an email address to register on the Knowledge Network. Information collected from users/system administrators in order to access the system, consists of user credentials (i.e. email address/username, password and google authenticator).

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

Mailing Address

Phone Numbers

user credentials

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

SAMHSA Grantees

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose for collecting PII is for registration, identification and notification to access and use the Knowledge Network.

The PII obtained from Administrators include name and email address in order to create account credentials and access to the system.

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

Not applicable.

Identify legal authorities governing information use and disclosure specific to the system and program.

SAMHSA: Public Health Service Act, Sections 301, (42 U.S.C. 241), 303 (42 U.S.C. 242(a), 322 (42 U.S.C. 249(c), 501 (42 U.S.C. 290aa), 503 (42 U.S.C. 290aa-2), and 505 (42 U.S.C. 290aa-4).

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.

09-09-0018

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

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.

A notice is provided upon account creation and login and requires acceptance of the terms that their personal information will be collected. The notice includes a Privacy Policy Endorsement Disclaimer by U.S. Government or SAMHSA. The user can contact U.S. Department of Health & Human Services with questions or comments.

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.

Currently there is no opt-out process is in place. If a user does not wish to provide the requested information, they can cancel their registration. Without providing name, email address, and business address; the user cannot register for or access the system.

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

There is no consent process in place for notifying individuals of major changes to 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 have the ability to update their own PII within the system. Issues that arise may be sent to the support email account listed on the site (info.privacy@samhsa.hhs.gov) and it will be routed to the Privacy officer.

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

In this initial pilot phase rollout of the system, there is no automated process to notify users to review their information. A manual process could be implemented to send out an email to all registered active users to review their information on a specific date.

To ensure PII data integrity, availability, accuracy, a number of technical controls are in place. They include audit trail, logging and logical access controls restricting access based on least privilege. Other technical controls include use of HHS computer involving two factor authentication and PIV card by administrators.

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

Users:

Users have access to their own PII to make any necessary updates. They do not have access to any other individual's PII.

Administrators:

Administrators may need to run reports and metrics.

Contractors:

Direct contractors have access to Knowledge Network to perform development, content editing, and user administration.

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

A limited number of Administrators will have access to user account and related PII only to perform maintenance and support activities. This is defined by their system role. There is no direct user to user contact facility in the application.

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.

Only administrators and authorized users have access to PII stored on the system. Access to the PII in the system is limited by role, based on the principle of 'Least Privilege'

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.

SAMHSA administrators, contractors and developers receive DHHS Privacy and DHHS Security awareness training when on boarded.

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

No training provided to users (above and beyond general security and privacy awareness training).

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.

Retention and destruction are covered under the schedule General Records Schedule1.1 item 011 under Financial Management and Reporting.

Retention is 3 years per schedule and destruction is 3 years.

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

Administrative controls include proper training by completing HHS Security Awareness training, signing HHS Rules of Behavior and proper on boarding following HHS rules.

Technical controls include audit trail, logging and logical access controls restricting access. Other technical controls include use of HHS computer involving two factor authentication and PIV card.

Physical controls include use of a PIV card as valid identification. In addition Knowledge Network is hosted on the Amazon Web Services government cloud. AWS provides physical security. From physical perspective, access to hardware housing PII data is in a secured facility, with only designated personnel having access. Physical access to the datacenter facility is secured by a multifactor authentication, including access to the general facility, separate keycard access to the office space housing the datacenter, and a separate cypher lock access to the datacenter itself. AWS maintains visitor logs for non-employees.

Identify the publicly-available URL:

https://knowledge.samhsa.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.

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