US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/10/2017

OPDIV:

SAMHSA

Name:

SAMHDA Data Portal

PIA Unique Identifier:

P-2453792-591609

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Design

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?

No

Identify the operator.

Contractor

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 Substance Abuse and Mental Health Data Archive (SAMHDA) Data Portal (DP) provides approved researchers access to restricted data files that are collected within the Center for Behavioral Health Statistics and Quality (CBHSQ) within the Substance Abuse and Mental Health Services Administration (SAMHSA).

The functions of the Substance Abuse and Mental Health Data Archive (SAMHDA) Data Portal are to provide approved researchers with access to National Survey on Drug Use and Health (NSDUH) and Drug Abuse Warning Network (DAWN) restricted data (collected within the Center for Behavioral Health Statistics and Quality (CBHSQ) within the Substance Abuse and Mental Health Services Administration (SAMHSA) files for the purpose of conducting custom analyses, support the process of analysis by providing statistical software tools, and further support analyses and report writing with Office software.

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

The Data Portal is not a data collection system. There is no website or data collection carried on through the Portal.

There are two types of information stored in the system.

The first type is personally identifiable information (PII) gathered from Data Portal users and RTI contractors, via the SAMHDA website, to allow access to the system. The PII consists of Name, Email address, Telephone number, Business Address, User-name, and password. These are voluntarily submitted when the application to use the Data Portal is made.

There are no direct contractors using the Data Portal, and RTI contractors do not us HHS Credentials to use the system.

The second type of data are the confidential data files from surveys performed by HHS Agencies on the state of mental health and substance abuse in the Nation. The data files are collected by the Center for Behavioral Health Statistics and Quality (CBHSQ). Researchers are given controlled access to the confidential and restricted data files through the SAMHDA Data Portal.

The researchers are not direct or indirect contractors, and users do not use HHS credentials to gain access, but rather complete a two-factor authentication process using the Junos Pule software.

As part of the application, the researcher(s) must determine which surveys and survey years are needed for the proposed project. The data currently available are for the National Survey on Drug Use and Health (NSDUH) and the Drug Awareness and Warning Network (DAWN). The survey years that are available are listed on the application. In addition, for a subset of more sensitive items, the researchers must include those items on their application and provide a research justification.

When the research application is approved, RTI moves a copy of each approved data file from a moderate security repository to the users' folder within the Data Portal file structure. Any requested sensitive items are included in the file; any such items not approved in the application process are not included.

PII is collected from users/system administrators to provide access the system, and consists of user credentials (i.e., user name, name, password, and email address). Users/system administrators include direct contractors from RTI and authorized researchers approved by SAMHSA. Users are issued login credentials that include user name and password.

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

The Data Portal is hosted by the direct contractor RTI, and is a secure remote computing environment for authorized researchers to access SAMHSA restricted data.

Users are research teams who have been approved by SAMHSA through a detailed application process. For SAMHSA to review the applications and respond to the researchers, Name, Email address, User-name, Telephone, Business Address, and password are collected on the SAMHDA website.

RTI contractors must provide Name, Email address, User-name, and password to be granted access to the Data Portal to administer the environment. Access depends on having an RTI moderate security account, which is granted after an extensive vetting and monitoring processes. RTI contractors do not use HHS credentials to access the Data Portal environment.

Approved users must complete the annual Data Confidentiality Training as specified by CBHSQ and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) training as specified by law. Each research user must sign either an Affidavit of Nondisclosure or Declaration of Nondisclosure:

Team members not Federal employees must sign and have notarized a Designation of Agent and Affidavit of Nondisclosure form where he/she agrees to abide by CIPSEA requirements and the Confidential Data Use and Nondisclosure Agreement.

If the researcher is a Federal government employee, the team member must sign the Designation of Agent and Declaration of Nondisclosure form after completing confidentiality training.

All researchers are required to have a data security plan backed by their institutions and must agree to site visits, as specified by the law and by CBHSQ.

Researchers are issued user names, passwords, and two-factor authentication tokens to access the Data Portal (DP) once they are approved. The DP is accessible only from approved computer physical location(s) and IP address(es) at researchers' organizations.

As part of the application, the researcher(s) must determine which surveys and survey years are needed for the proposed project. The data currently available are the National Survey on Drug Use and Health (NSDUH) and the Drug Awareness and Warning Network (DAWN). The application lists the survey years available. For a subset of more sensitive items, the researchers must include them on their application and provide a research justification.

When the research application is approved, RTI moves a copy of approved data files from a moderate security repository to the users' folder within the Data Portal file structure. Any requested sensitive items are included in the file; any such items not approved in the application process are not included.

The NSDUH and DAWN data files are used by the researchers by submitting them to statistical programs written in one of the statistical packages (such as SAS) which are available in the Data Portal to researchers. These packages provide the user with aggregated descriptive and statistical information about the file as specified in their statistical programs.

Users are required to maintain the confidentiality of the data in the Data Portal. Researchers cannot transfer data into or out of the Data Portal by any method, including cut and paste. Researchers may perform analysis within the portal using approved data and statistical packages to access and analyze restricted data. No results can be removed until they are reviewed for PII by the SAMHDA Contracting Officer's Representative (COR). If approved, RTI removes and securely transmits the materials to the researcher.

PII is collected from users/system administrators to provide access the system, and consists of user credentials (user name, name, password, telephone, business address, and email address). System administrators include direct contractors from RTI. Authorized researcher users are approved by SAMHSA. Users are issued login credentials that include user name and password.

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: PII is collected from the Users and the Administrators to enable them to access

Restricted use NSDUH and DAWN data files.

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

Public Citizens

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is collected from users/system administrators to provide access the system, and consists of user credentials (i.e., user name, name, password, and email address). Users/system administrators include direct contractors from RTI and authorized researchers approved by SAMHSA. Users are issued login credentials that include user name and password.

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

The PII collected by the system is used for authentication purposes only. There are no secondary uses. The PII contained in the restricted use data files is used by researchers for research. Researchers will not be retrieving individual PII records at all. All restricted use data files are analyzed at a higher level than individual PII records.

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

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) Title 5 of Public Law 107-347 – This act protects data collected for statistical purposes, by Statistical agencies or units that directly acquire information from respondents, including state and local governments. It also allows for these statistical agencies/units to designate agents to acquire information for the agency under CIPSEA as well as perform other exclusively statistical activities for the agency on CIPSEA protected information. 42 USC § 290AA – This law protects all other data collected, that is not covered by CIPSEA. It clearly states that the person, or establishment that provides the data shall not be identified. It also states that any of this data/information collected may not be published or released (unless consent is given), and will not be published/released in a way that allows respondents to be individually identified. The law also states that data will only be used for the purpose for which it was collected and agreed upon by the respondent.

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.

HHS agency wide SORN; 09-90-1401 Records About Restricted Dataset Requesters.

Identify the sources of PII in the system.

Email

Non-Governmental Sources

Public

Private Sector

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.

All Data Portal users are given prior notice that they must submit PII as part of the application process. Data Portal users are researchers who must submit a detailed application for access to the Data Portal that includes their name, email, telephone number, and business address.

The application also provides details of the research being carried out. Applicants understand that they must submit PII during the application process or their application will not be accepted.

RTI contractors are notified that they must submit their PII to be granted access. This is a requirement of employment to work on the project.

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.

Potential Data Portal users are informed of the requirement to submit PII and information on their research in the application process. They may opt out of providing their PII and not submit an application for access to the Data Portal.

RTI contractors are notified that they must submit their PII to be granted access. If they choose not to submit PII, they are removed from the project. Submitting PII for Data Portal access is a requirement of employment to work on the project.

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

Submission of PII to access the Data Portal is fully voluntary.

There are no plans to make disclosure or data use changes to the system that would invalidate the original reason for collecting PII. If any changes are made to the system, users are notified via email prior to the change; they may consent to the change or they may withdraw their PII and give up their access to the Data Portal.

RTI Contractors submit PII as a condition of employment. If any changes are made to the system, they are notified via email prior to the change; they may consent to the change or they may withdraw their PII and give up their access to the Data Portal.

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.

Researchers voluntarily submit PII during the application process to be granted access to the Data Portal If at any time they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, they may contact SAMHSA to have their PII updated and/or express any other concerns regarding their PII. Researchers are provided contact information during the application process.

RTI Contractors supply their PII as part of Terms of Employment, and provide them voluntarily. If they believe their PII has been mishandled, they notify the Data Portal project management to express their concerns or have their PII updated.

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

To ensure they are relevant and accurate, the project's Contracting Officer's Representative (COR) manually reviews the information collected through voluntary submission by Researchers of PII during the application process.

These reviews of information for integrity, availability, and accuracy and relevancy are performed by SAMHSA on the applications received from Researchers and their PII.

SAMHSA sends an annual email requesting that Researchers review their information and ensure that it is accurate and up-to-date. To ensure relevancy, if users provide any updates, system administrators change the individuals' information accordingly. Data Integrity is maintained through user access recertification and encryption for data at rest and in transit.

In addition, reviews are performed by RTI project management on the direct contractors (developers and administrators) on the project.

To ensure availability, RTI has back-up servers to ensure information is readily available, even if a main server fails.

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

Users:

Researchers are granted access only to restricted use data files for which they have received SAMHSA approval to analyze. While the individual PII records are within the restricted use data files, researchers are required to run their analyses at the aggregate level and not at the individual level.

Administrators:

To provide access to the system and provide user credentials.

Developers:

Have access as a part of the development process.

Contractors:

The Administrators and Developers are RTI contractors to SAMHSA on the project and must supply PII as terms of their employment and to gain access to the system to perform administrative functions and maintain the environment.

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

Access to PII is role-based. Data Portal administrators are granted privileges that allow them to access only functions and information necessary for their role.

RTI contractors are granted limited privileges by the RTI Moderate Network administrators that allow them limited access to the infrastructure to work on the application.

When RTI designs a system, the project team understands and identifies what activities are required to develop, test, deploy, and maintain the system in the hosting environment. Based on that understanding, project management identifies the team individuals and the roles and access they need to perform the duties and activities required. After this determination is made the project team requests the required access from SAMHSA's Division of Technology Management (DTM).

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.

Access to PII is role-based. RTI Data Portal administrators are granted privileges that allow them to access only functions and information necessary for their role.

RTI contractors are granted limited privileges by the RTI Moderate Network administrators that allow them limited access to the infrastructure to work on the application.

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.

The RTI contractors take the HHS Privacy Awareness training as well as HHS Information Systems Security Awareness Training; they also are required to take RTI IT Security Awareness Training annually. RTI contractors also read and sign the RTI Rules of Behavior. Researchers must complete Data Portal Confidentiality Training. Each team member must complete the online Data Portal Confidentiality Training course and read the approved Application for Access, Confidential Data Use and Nondisclosure Agreement (CDUNA), and the Data Portal Confidentiality Procedures Manual. Each team member must sign either an Affidavit of Nondisclosure or a Declaration of Nondisclosure. Each team member who is not a Federal employee must sign a Designation of Agent and Affidavit of Nondisclosure form where he/she agrees to abide by CIPSEA requirements and the Confidential Data Use and Nondisclosure Agreement. This Affidavit must be notarized. If the research team member is a Federal government employee, the team member must sign the Designation of Agent and Declaration of Nondisclosure form after completing the confidentiality training.

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

The RTI contractors also participate in the SAMHSA Records Management 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.

The PII collected in voluntary submission during the application process from Researchers is kept for the length of the contract or deleted upon user request.

In addition, SAMHSA and Office of Personnel Management (OPM) records schedules apply, which may include National Archives and Records Administration General Records Schedule 20 - Electronic Records- as well as other applicable SAMHSA schedules. At this time SAMHSA is in a review to update the current records schedule and this PIA will reflect that update upon approval.

The PII collected from the RTI contractors for administrative access is kept in accordance with RTI Policy 1.9, Records Retention, for a minimum of 6 years or as dictated by contract or applicable federal regulation.

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

Physical: The physical location of all data, servers and archives pertaining to the Data Portal are in locked secure facilities provided by RTI contractors and by SAMHSA and the federal government.

RTI's data centers and campus facilities are accessible to authorized staff only via a key card.

Administrative: RTI contractors generate audit records when PII is placed in the system, when new website content is processed, and when Researchers log in and perform activities.

Audit records are reviewed by appropriate staff (e.g., the system administrator reviews Researcher activity) on a routine basis. Audit records are time-stamped by the system, and reside in a database system which is not writable by most staff. Audit records are kept in perpetuity of the contract. Firewalls and anti-virus software are also used to mitigate risks, and protect data integrity.

Technical: The PII is secured using Moderate Impact security controls based on the National Institute of Standards and Technology (NIST) 800-53 document and role-based access specific to the authenticated user.