

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/30/2016

OPDIV:

SAMHSA

Name:

Rapid HIV/Hepatitis Testing

PIA Unique Identifier:

P-8650082-019105

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Test

null

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

Yes

Identify the operator.

null

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.

PIA Validation (PIA Refresh/Annual Review)

Describe the purpose of the system.

This is a web-based data collection portal used by Substance Abuse and Mental Health Services Administration (SAMHSA) Human Immunodeficiency Virus (HIV) grant programs to enter data and used by government project officers (GPO's) to monitor grant performance. Data is verified and validated using logic checks and then used to run customized system generated reports to respond to SAMHSA's reporting requirements which tracks the effects and accomplishments of its HIV grant programs for HIV and Hepatitis screening treatment and substance abuse (SU) treatment services.

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

The client level data collected pertains to health risk indicators such as alcohol use, drug use, sexual risk history, and HIV status to identify those individuals in need of substance use (SU) treatment, HIV medical care referral services, and other wrap-around case management services. Grantees enter de-identified client data using computer generated client ID to track client outcomes at intake and follow-up and to prevent duplicate counts in reporting. The data that is collected is de-identified prior to entry into the system. This process is done when the grantee assigns a random number that does not link back to any particular individual or identify any PII data within this system that captures aggregated data. The client ID does not capture any of the sensitive personal identifying information. No client names, emails, social security numbers, or address are collected or stored in the system.

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

System users (grantees and GPO's) information (name, work phone number, email and work addresses) are stored in the system and are used for authentication purposes only during log-in for data entry. The client level information is captured and used for the required reporting purpose. This client level data will reference to health risk indicators such as alcohol use, drug use, sexual risk history, and HIV status to identify those individuals in need of substance use (SU) treatment, HIV medical care referral services, and other wrap-around case management services. This user information is not shared with any other system.

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

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

Employees

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

Authentication for system user account access at log-in.

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.

Departmental Regulations 5 USC 301

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.

SORN is In Progress

Identify the sources of PII in the system.

Email

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

OMB No. 0930-0343

Expiration Date: 09/30/2017

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.

Notice is not provided as this information is part of their grant application to SAMHSA. Only updated information is retrieved from the Project Director when personnel changes occur and are approved at SAMHSA by grants management specialist and the government project officer.

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 cannot object to the collection or use of their PII because data collection and reporting is a requirement of all grant applications at SAMHSA.

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

If a major change to the system occurs, users will be notified through email notification originating from the ABT and Associates Help Desk. The change will be described and consent will be implied unless the user responds to the email with a specific request.

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.

If a user believes their contact information has been inappropriately obtained by the system, used, or disclosed, the user may contact the Help Desk and register a comment or complaint. If a complaint is registered, it will be escalated immediately through ABT and Associates management to SAMHSA's contracting officer representative (COR) and Privacy Officer for processing and resolution.

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

ABT and Associates receives information about the user data accuracy and availability directly from users through ABT's Help Desk when a problem is detected. If a user finds their contact information has been incorrectly entered into the system, the user will contact the Help Desk to have the information corrected. The integrity and availability of the information is maintained by the information system controls at the application level and put in place in the GovCloud hosting environment.

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

Users:

The users (grantees) will have access to the system as they are the entering the data into the. The GPOs will monitor the performance based on the data entered into the system.

Administrators:

The system administrators will have access to allow to make changes when new grants are awarded or when a change in personnel occurs.

Contractors:

The contractors will have access to the system as they are in place at various levels to assist will trouble shooting and also knowledge management to assist the GPOs if needed.

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

Access to the PII in the system is limited by role: only SAMHSA and ABT's staff members with Administrative or Low Administrative privileges are allowed access to the PII. These roles and access are approved by the SAMHSA Contracting Officer Representative (COR) and ABT's Project Management on a case by case basis.

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 SAMHSA and contractor staff members who will access the PII are granted Administrative or Low Administrative privileges and are approved by the SAMHSA COR and ABT's Project Management on a case by case basis. The system uses administrator-defined user groups to restrict access by role. A project system manager will create and maintain appropriate user identification groups.

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 contractor staff members who will access the system receive security awareness and ethics training immediately upon employment and annually thereafter. Among the topics addressed are: Definitions; Rules of behavior; Access Controls; Email Security; Internet Security; Secure Data Storage; Information Security Incidents; HIPPA Compliance for Business Associates; Insider Threats; and Additional RTI Resources. SAMHSA personnel are required to take and maintain HHS Information Systems Security Awareness Training.

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

All new users are offered training before access is granted. Periodic refresher trainings are offered to existing users. The users/access members will have Privacy Awareness training to include that of HHS rules of engagement training. Refresher training will be captured on an annual basis and recorded for each individual having access.

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.

PII collected through the System will remain on secured server(s) until a request is made to move/remove/transition or destroy data at the end of the contract. ABT maintains records for the time frames specified and destroys records in accordance with all applicable federal laws and regulations and in accordance with Retention, Storage, Retrieval, and Destruction of ABT's Records. This is covered under GRS 3.2, Item 010.

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

The system will be housed in the SAMHSA GovCloud environment, which protects the confidentiality, integrity, and availability of data through the application of administrative, technical, and physical controls that meet the appropriate SAMHSA-directed impact level of the data. Standard access security features include user identification and password, lockout of account upon repeated entry of an invalid password, file- and directory-level security, periodic backups, anti-virus software, and administrator-defined user groups. At the application level, the system uses user identification and password, lockout of account upon repeated entry of an invalid password and other security measures.

Identify the publicly-available URL:

The URL will be determined and provided after the Authorization To Operate (ATO) is final.

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?

No

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