US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/08/2017

OPDIV:

SAMHSA

Name:

Program Evaluation for Prevention Contract

PIA Unique Identifier:

P-4130704-883429

The subject of this PIA is which of the following?

Major Application

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.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

Internal Flow or Collection

Add-on to the PEP-C system.

Describe in further detail any changes to the system that have occurred since the last PIA.

The system now includes a new data collection for the Strategic Plan Framework-Prescription Drug Misuse (SPF-Rx) which will be added to the Program Evaluations for Prevention (PEPC). This includes data collection instruments that are very similar to the Partnerships for Success-- grantee and community level data. The modules will be an add-on to the PEPC system.

Describe the purpose of the system.

The PEPC system will house cross-site data for the Minority AIDS Initiative (MAI), SPF-Prescription Drugs , and Partnerships for Success (PFS). The purpose of all three programs is to determine if and how the implementation of the Strategic Prevention Framework (SPF) results in improved intermediate, short, and long-term outcomes. These outcomes may include reduction in HIV cases, reduced substance misuse, and reduction or prevention of opioid misuse. The purpose of the data are for Government Performance Reporting Act (GPRA) reporting and to show program impact. The evaluation is being performed within the PEPC umbrella contract (staff are contractors). PEPC staff work with SAMHSA’s grantees to collect data and provide related training and technical assistance.

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

For MAI, PEPC will receive two types of data from grantees to use in the cross-site evaluation. (1) Client survey data – the grantees upload surveys completed by the adult or adolescent client receiving substance abuse and/or HIV/Hepatitis related services. Clients who receive services complete surveys appropriate to the level of services they receive and report on their substance use and HIV-related knowledge, attitudes, beliefs, and behaviors. The data will not include personally-identifiable information. This type of information is collected to assess change in behavior over time. (2) The grantees also upload service utilization dosage forms documenting the types of services (e. g.. counseling, education) received by clients and the duration of each type of service. No personally-identifiable information is on the dosage forms and they are not linked back to individuals in any way. In submitted evaluation reports, client survey and dosage form data are provided only at the aggregate, not individual, level. PEPC collects grantee and sub-grantee input data and reports on current and future cross-site evaluation activities. The PEPC system contains PII of the system's grantee users only as needed to contact them for the purposes of managing the grant program. The name, email, and telephone phone numbers are in a database for PEPC.

For PFS and SFP-Rx, the data instruments include the community level and grantee level questions. Grantees can only see their own information, which includes the personnel under their supervision. Only cross-site roles (e.g. Project Administration, Data Processing) can see contact information for all users. These are restricted roles issued only to the SAMHSA Contracting Officer Representative (COR), the Project Director, Project Administrator, and active cross-site staff at RTI. The same PII elements are collected for all users of the system, including SAMHSA employees and contractors.

The system does collect name, email, and contact telephone for SAMHSA users as well as RTI employees to control access. RTI contractors are non-Direct contractors and do not use any HHS credentials.

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

Grantees will continue collecting and compiling community level and participant-level survey data using the PEPC system as appropriate. The HIV data will include client level data on HIV and substance use behavior. The PFS and Rx instruments will collect data on underage drinking and/or prescription drug misuse at the community level. Grantees will continue collecting and compiling community level and participant-level survey data using the PEPC system as appropriate. The HIV data will include client level data on HIV and substance use behavior. No Personally Identifiable Information is collected here. The PFS instruments will collect data on prescription drug misuse and underage drinking at the community level. This data is aggregated and contains no Personally Identifiable information. Data is collected for analysis and evaluation purposes. Data are analyzed to show program impact and report GPRA data.

The PII information that is collected by the system is the name, email and contact telephone numbers of the users that login to the system. These data elements are collected to provide access to the system and are stored only through the life of the project. Username and Password are used to grant access to the 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

Phone Numbers

User Credentials.

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?

500-4,999

For what primary purpose is the PII used?

The primary purpose of the user credentials are so the grantees can access the system. The secondary purpose of the user credentials are so PEPC and RTI can follow-up with grantees via email and phone to address data issues and provide system training. The PII is used administratively to allow the Contract Officer's Representative at SAMHSA, SAMHSA Project Officers, and active cross-site staff at RTI to maintain contact with Grantees to ensure that the data are collected appropriately and for Grantees to maintain contact with sub-recipients to ensure that contractual requirements are being met.

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

None. The data is only used administratively.

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

Established in conformance with the Public Health Service Act, Anti-Drug Abuse Act of 1986, the Omnibus Anti-Drug Abuse Act of 1988, and the ADAMHA Reorganization Act of 1992.

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 09-30-0027 Grants and Cooperative Agreements.

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Private Sector

Other

Identify the OMB information collection approval number and expiration date

PFS--OMB No. 0930-0348. Expiration Date 04/30/2018
MAI--OMB No. 0930-0298 Expiration Date 03/31/2019
SPF-Rx OMB: currently under the 60 FRN until June 14

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.

The process in place to notify grantees that their personal information will be collected is an email sent directly to the grantee. Personal information is required to manage and report on the Grants programs.

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.

There is no opt out process for the system. The information is required of all users to carry out their assigned duties. For Grantees it is a condition of participation in the Grants program. For participating SAMHSA employees and contractors it is needed for delivery of notifications to and from Grantee and other users, as well as the provision of assistance as needed.

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

There are no processes in place to obtain consent from individuals whose PII is in the system when major changes occur to the system. Only changes to the system that do not contradict the initial consent of the individual are allowed. Major changes that would void the initial consent will not be implemented. The PII in the system is for Grantee contact purposes, and to grant user and administrator access.

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 system users find that their PII is inaccurate, they have the ability to correct it themselves within the System. Alternatively, they may contact their Grantee, their SAMHSA Project Officer, or PEP-C Technical Assistance staff and request the updates to be made on their behalf. If there is a breach or similar security incident, the individual would report this as soon as it is discovered and the breach would be handled under the Incident Response Plan.

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

User-supplied PII is reviewed on a quarterly basis as part of the mandatory progress reporting and review process. Grantees and SAMHSA Project Officers are also in regular communication with each other, and occasionally with other PEP-C project staff, to maintain the accuracy of contact information as a normal part of administering the grant programs. User-supplied PII is reviewed on a quarterly basis by communication between Grantees and SAMHSA Project Officers in addition to RTI PEP-C project staff, to maintain the accuracy of contact information as part of grant program administration. The PII is maintained by RTI in the following manner:
Integrity: An audit log system ensures the PII data protected in RTI’s Moderate Network and the PEP-C system has not been improperly accessed, modified, or destroyed.
Availability: The availability of all PII is protected by the RTI Moderate Network security controls in place and access is restricted to authorized users among the project team.

Accuracy and relevancy: PII of grantees is reviewed by SAMHSA Project Officers in conjunction with the Grantee for accuracy and relevancy. Grantees and sub-recipients are permitted access to only their own PII and that of anyone for whom they have administrative responsibility

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

Users:

Grantee users must maintain contact information for their staff and sub-recipient users. All grantees and sub-recipients are permitted access to only their own PII and that of anyone for whom they have administrative responsibility.

Administrators:

The SAMHSA COR must maintain contact information for their grantees to administer the grant agreement. SAMHSA Project Officers have access only to those grantees for whom they have administrative responsibility, and cannot access PII of other grantees.

Developers:

Certain system developers must have access to ensure the system is working correctly and as intended.

Contractors:

The Developers are contractors for SAMHSA and host and run the website (They are not Direct Contractors). Please see Developer access to PII.

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

Contractor RTI and SAMHSA employ National Institute of Standards and Technology (NIST) 800-53 Rev 4 controls, including the Personnel Security controls, to ensure that users are appropriately identified, undergo requisite background screening, and are cleared for the risk level and sensitivity level required for their roles.

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 PEP-C system employs NIST 800-53 Rev 4 controls to ensure that access to any data is restricted by role. AC-6 requires the use of least privilege, allowing only authorized access for users that are necessary to accomplish assigned tasks in accordance with SAMHSA mission and business functions.

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.

RTI requires all personnel to complete the company-wide, IT security awareness training before obtaining authorization to access the information system. RTI offers this training within 30 days of employment and a refresher course at least annually thereafter so the users can maintain their access. Additionally, users must complete training - specifically HHS Annual Privacy Awareness Training, but not Information Systems Security Awareness Training - when required by SAMHSA or when major information system changes take place.

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.

The National Archives and Records Administration (NARA) is determining the appropriate, Records Control Schedule (RCS), and Job Number or General Records Schedules (GRS) for some or all of the PII maintained in the system and that the PII should be maintained until a determination is provided. The project maintains and disposes records in accordance with applicable HHS policy and procedure, all contractual requirements, and RTI Policy 1.9 Retention of Electronic Records, which requires storage of project files and data for 6 years past the end of the project date.

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

Administrative- Records are maintained according to specific records control schedules and policy. PII is secured administratively by role-based access that limits information visibility only to those authorized to see it.   Technical-The PII is secured using Secure Socket Layer (SSL) during transmission and form authentication with role-based access specific to the authenticated user. Physical: Access to the servers is protected via multi-level key card and code access. RTI's Data Center is certified at level Federal Information Processing Standard (FIPS)-Low or higher.

Identify the publicly-available URL:

https://pep-c.rti.org

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