Privacy Impact Assessment (PIA): SAMHSA - PEP-C - QTR3 - 2023 - SAMHSA1527274

Created Date: 10/18/2023 12:06 PM Last Updated: 1/5/2024 10:47 AM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	SAMHSA - PEP-C - QTR3 - 2023 - SAMHSA1527274	**PIA ID:**	1722767
Name of Component:	SAMHSA - SAMHSA - SAMHSA - Program Evaluation for Prevention Contract	**Name of ATO Boundary:**	Program Evaluation for Prevention Contract
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	68
Submission Status:	Submitted	**Submit Date:**	9/28/2023
Next Assessment Date:	N/A	**Expiration Date:**	12/4/2026
Office:	SAMHSA	**OPDIV:**	SAMHSA
Security Categorization:		**OpDiv PIA ID:**	SAMHSA1527274
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Development
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	1/12/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The data collection system changed from a DNN (DotNetNuke),framework to DotNet6.0. The requirements remained the same, but the overall design and underlying architecture of the system has been modified
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	PEPC (Public Engagement Platform) is a Web-based application which is a national cross-site evaluation of (SAMHSA-Substance Abuse and Mental Health Administration) Strategic Prevention Framework for Prescription Drugs (SPF Rx). It includes program monitoring, process evaluation, and outcomes evaluation activities. The PEPC team develops and manages online systems to collect program data from SPF Rx grantees and their communities and to gather and manage large prescription-drug-related administrative data sets. Tasks include developing an OMB (Office of Management and Budget) package and evaluation and data processing plans, conducting analyses, and developing evaluation reports and presentations

PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The system collects the name, email, and phone number of individuals who are granted access to the system
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	The information collected is used to create user accounts to allow grantees to access the system. The secondary purpose is to allow PEPC and the contractor to follow up with grantees via email and telephone to address system issues as needed and to provide training. The PII (Personally Identifying Information) is used administratively by the Contract Officer's Representative at SAMHSA, by Government Project Officers, and active cross-site staff at the contractor to maintain contact with Grantees. Grantees maintain contact with sub-recipients to ensure that contract requirements continue to be met.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Purpose: The PEPC team develops and manages online systems to collect program data from SPF-Rx grantees and their communities and to gather and manage large prescription-drug-related administrative data sets Access: 21 Grantees and their Subrecipients who are part of the SPF Rx 2021 cohort will have access to the website via a URL (Uniform Resource Locator) and login
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	No
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	

PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Grantees Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The system collects the name, email, and phone number of individuals to create accounts on the system and allow them access to the system
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses of the PII (Personally Identified Information)
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The project is in conformance with the Public Health Service Act, Anti-Drug Abuses Act of 1986, the Omnibus Anti-Drug Abuse Act of 1988, and the ADAMHA (Drug Abuse, and Mental Health Administration) Reorganization Act of 1992. The System of Records Notices (SORN) is Grants and Cooperative Agreements: Alcohol, Drug Abuse, and Mental Health Services Evaluation, Service, Demonstration, Education, Fellowship, Training, Clinical Training, and Community Services
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Email Address
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	SORN 09-30-0027 Grants and Cooperative Agreements
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	Office of Management and Budget (OMB) number: 0930-0377
PIA - 10B:	Identify the OMB information collection approval number expiration date.	12/31/2025
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Not Applicable
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can 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. The information is required of all users to perform their assigned duties. For Grantees it is a condition of participation in the Grants Program. For SAMHSA (Substance Abuse and Mental Health Administration) employees and contractors on the program it is needed to deliver notifications to and from Grantees and other users, and to provide assistance as needed.

PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	There is no process in place to obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Only changes that do not contradict the initial consent of the individual are allowed. Major changes that would void the initial consent will not be implemented.
PIA - 15:	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 no process exists, explain why not.	If a system user finds there PII is inaccurate, they have the ability to correct it themselves in the PEPC (Public Engagement Platform) system, or they may contact their Grantee, their SAMHSA Project Officer, or PEPC Technical Assistance Staff and request and update. If there is a breach or similar security incident, the individual would report this as soon as it is discovered, and it would be managed under the Incident Response Plan
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	User PII is reviewed on a quarterly basis as part of the mandatory progress reporting and review process to maintain the accuracy of contact information as part of the grant program administration. Grantees and SAMHSA Project Officers are also in regular communication, and also communicate with other PEPC staff, to maintain accurate records. The PII is maintained by RTI (Research Triangle Institute) as follows: Integrity: audit logging ensures that PII is protected in SAMHSA's Moderate GovCloud (Government Cloud) and the PEPC system and that it has not been improperly accessed, modified, or destroyed. Availability: The availability of the PII is maintained by the SAMHSA's Moderate GovCloud security controls in place and access is restricted to authorized users among the project teams. Accuracy and relevancy: PII of Grantees is reviewed by SAMHSA Project Officers in conjunction with the Grantee to ensure accuracy and relevancy. Grantees and sub-recipients can access only their own PII and PII of anyone for whom they have administrative responsibility
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users are Grantees who must maintain contact information for the staff and subrecipient users. · Administrators are RTI employees and have role-based access to system information as part of their role in maintaining the system data base and to ensure the system is working correctly and as intended. · Developers are RTI employees and have role-based access to system information as part of their role in maintaining the system data base and to ensure the system is working correctly and as intended. · RTI project team employee (contractor) has access to the system to conduct their defined work on this task, none can change their access information without going through an Administrative process
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The RTI project team uses National Institute of Standards and Technology (NIST) 800-53 controls to ensure that only those individuals authorized to access the data are allowed to access the system. RTI employs NIST 800-53 Rev 4 controls, including the Personnel Security controls, to ensure that project team members are appropriately identified, undergo requisite background screening, and are cleared for the risk level and sensitivity level required for their roles. In addition, RTI personnel are identified at the project level by role, and only appropriate personnel with the requisite skills and knowledge are assigned to a project in the required role
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	The PII is secured using role-based access determined by roles assigned by project management to personnel along with appropriate privileges for accessing the network and data to complete their role on the project. Secure Socket Layer (SSL) is used during data transmission as well as when submitting form authentication with role-based access specific to the authenticated user.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.	Users receive RTI Information Security Awareness Training upon hire and annually thereafter, as well as Privacy Awareness Training and other RTI required trainings annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	In addition to security awareness training, RTI personnel receive training on use, integrity, and storage of data and the methods of individuals to report potential issues to RTI staff and compliance officials.

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The project maintains and disposes of records in accordance with applicable HHS (Health and Human Services) and SAMHSA 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. The National Archives and Records Administration (NARA) is determining the appropriate Records Control Schedule (RCS) Job Number or General Records Schedule (GRS) for some or all of the PII maintained in the system and that the PII should be maintained until a determination is provided
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative: Records are maintained according to specific records control schedules and policy as determined under the contract and by SAMHSA. 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 servers is protected via multilevel keycard and code access. Access to RTI physical campus is protected via keycard and code access, and SAMHSA's AWS (Amazon Web Services) servers are certified at FIPS (Federal Information Processing Standards) Moderate.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/28/2023
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	System is in Production phase, not development. This cannot be changed as we are still having issues with the syncing between EA Now and Archer.	**SOP Review Date:**	10/18/2023
		SOP Days Open:	20

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/19/2023
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski All comments have been addressed, this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per email back and forth with SAMHSA, next iteration can update the Sensitive PII question to: No.	**SAOP Review Date:**	12/5/2023
		SAOP Days Open:	47

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
RE_ PIA_ SAMHSA - PEP-C - QTR3 - 2023 - SAMHSA1527274.pdf	156332	.pdf	11/17/2023 2:40 PM	1

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	LASKOWSKI, JAMES	10/19/2023	Per PTA-5B, username and password are used to access the system. Please add username and password to your response.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	1/5/2024 10:47 AM	**History Log:**	View History Log