Privacy Impact Assessment (PIA): SAMHSA - PEP-v2 - QTR2 - 2024 - SAMHSA2052339

Created Date: 7/18/2024 12:05 PM Last Updated: 8/2/2024 3:55 PM

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-v2 - QTR2 - 2024 - SAMHSA2052339	**PIA ID:**	2031337
Name of Component:	SAMHSA - Public Engagement Program (PEP) - v2	**Name of ATO Boundary:**	Public Engagement Program (PEP) - v2
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	79
Submission Status:	Submitted	**Submit Date:**	7/3/2024
Next Assessment Date:	08/02/2027	**Expiration Date:**	8/2/2027
Office:	SAMHSA	**OPDIV:**	SAMHSA
Security Categorization:		**OpDiv PIA ID:**	SAMHSA2052339
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	2/3/2023
5:	Is the system or electronic information collection, agency or contractor operated?	

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.	Regular operation and maintenance Enhancement of security and user experiences (Drupal version upgraded to 10)
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.	The Substance Abuse and Mental Health Administration (SAMHSA) Store offers various publications and digital products at no cost to the public. These resources cover a broad spectrum of topics, including substance abuse prevention, treatment, recovery, and mental health issues. The store provides these materials in both physical and digital formats, with regular shipping of stocked items being free within the United States (U.S.) and its territories. The availability of items is indicated on the store's website, with some products being available only as digital downloads.

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 https://store.samhsa.gov/ collects and stores the names, addresses, phone numbers, and email addresses, which are shared with GPO (Government Printing Office) and are required to submit a free of-charge order of the resources. Operating Division(OpDiv) Employees and Contractors: OpDiv employees and contractors who need administrative access to the websites undergo background checks and approval from the System Owner and the Chief Information Security Officer (CISO). Once access is granted the admins are required to use (Government Furnished Equipment) GFE and 2-Step Verification (Personal Identity Verification (PIV)- and passcode).
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.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address HHS Username Password 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 provided by users voluntarily. It is used for delivering ordered products to the customers and for contacting the customers regarding any issues with the orders/stock inventory. Emails/usernames and passwords for the internal administrators are stored encrypted and protected by two-factor authentication when using government-provided equipment.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
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)?	Yes
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.	The store provides resources in both physical and digital formats, with regular shipping of stocked items being free within the U.S. and its territories. The availability of items is indicated on the store's website, with some products being available only as digital downloads. Resources are available to the public via public Uniform Resource Locator (URL); no login is required.
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?	Yes

PTA - 12:	Does the website use web measurement and customization technology?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not 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?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	HHS
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.	1. SAMHSA Disaster Mobile App - In a disaster, it's essential that behavioral health responders have the resources they need—when and where they need them. The free SAMHSA Disaster App offers first responders immediate access to any type of traumatic event at every phase of response, including pre-deployment preparation, on-the-ground assistance, and post-deployment resources. 2. Suicide Safe - For individuals at risk of suicide, primary and behavioral health care settings provide unique opportunities to connect with the health care system and access effective treatment. Suicide Safe is a free mobile app that helps providers integrate suicide prevention strategies into their practice and address suicide risk among their patients. The Suicide Safe app is based on SAMHSA's Suicide Assessment Five-Step Evaluation and Triage (SAFE-T) card. 3. AlchoholFX (available for tablets only) - Alcohol's Effects on the Brain (AlcoholFX) is a free, science-based app that teaches students ages 10 to 12 how alcohol can harm their brains if they drink. Based on lesson plans from SAMHSA's Reach Out Now Initiative, the app can easily integrate with instruction in 5th- and 6th-grade classrooms. This app is only available on tablets. 4. Talk. They Hear You. - "Talk. They Hear You." is a free mobile app that helps you prepare for one of the most important conversations you may ever have with your children about underage drinking. The app provides parents and caregivers of children and teens ages 9 to 15 with the tools and information they need to start talking with their children early about the dangers of alcohol. It includes a suite of materials that helps reinforce the underage drinking prevention campaign's messages.
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes

PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	Yes
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	Yes
PTA - 18:	Does the mobile application use measurement and customization technology?	Yes
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	Trackable Action occurs in the mobile application • Action triggers Amazon Web Services (AWS) Lambda via Application Programming Interface (API) Gateway Endpoint • Lambda function triggers a "Write-To-DB" where the information is written to an AWS Relational Database Services (RDS) (PostgreSQL) database • Database is connected to an AWS Quicksight Dashboard for Application Product Owners to leverage
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	Yes
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	No
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?	No
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	Yes
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 Mailing Address Other - Free text Field - IP addresses
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Name and shipping address is used to deliver orders Phone numbers and email addresses are used to send communication on delivery updates IP address is collected by the system and not used anywhere
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None
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 legal authorities governing information use and disclosure specific to the U.S. Department of Health and Human Services (HHS) include the following: Health Insurance Portability and Accountability Act (HIPAA) HITECH Act 42 CFR Part 2 Common Rule Federal Confidentiality Laws Medicare and Medicaid Laws
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
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.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB CONTROL NUMBER: 0930-0393
PIA - 10B:	Identify the OMB information collection approval number expiration date.	3/31/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	It is shared with The Government Publishing Office staff to fulfill the orders placed by public.
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)).	None
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.	The information collected are provided by users voluntarily. It is used for delivering ordered products to the customers and for contacting the customers regarding any issues with the orders/stock inventory. Emails/usernames and passwords for the internal administrators are stored encrypted and used for two factor authentication when using the government provided equipment.
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.	The Personally Identifying Information (PII) is collected to fulfill the product orders. The order cannot be delivered if the address is not provided.

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.	Store.samhsa.gov/PEP-2 is under the Health and Human Services umbrella, and like other government agencies, comply with relevant privacy laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Health Information Technology for Economic and Clinical Health (HITECH) Act, when handling PII. The specific requirements for notification and consent vary depending on the specific context of the system and the types of PII involved.

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.	Federal and State Data Breach Notification Laws SAMHSA is authorized under section 501(d)(16) of the Public Health Service Act Gather Information: When an individual believes there has been inappropriate obtaining, use, disclosure, or inaccuracy of their PII, they can contact the HHS Office for Civil Rights (OCR) to initiate the complaint process. The individual should provide relevant information, such as their name, contact details, a description of the incident, and any supporting evidence if available. Submit a Complaint: Individuals can submit their complaint through various means, such as by mail, email, or online via the OCR's official complaint portal. The OCR typically provides specific instructions on how to file a complaint on its website. Complaint Review: After receiving the complaint, the OCR reviews the details provided by the individual. They assess whether the complaint falls within the scope of the applicable privacy laws (e.g., HIPAA) and if there are sufficient grounds to proceed with an investigation. Investigation: If the OCR determines that the complaint is within its jurisdiction and raises valid concerns about a covered entity's (e.g., healthcare provider, health plan, or clearinghouse) privacy practices, they will initiate an investigation into the matter. Resolution or Enforcement: The OCR's investigation aims to identify any violations of applicable privacy regulations. If violations are found, the OCR works with the covered entity to address and resolve the issues. This may involve corrective actions, changes to policies and procedures, or other remedies to prevent future incidents. Notification: The OCR communicates with the complainant regarding the status and outcome of the investigation. If appropriate, they will inform the individual of any corrective actions taken by the covered entity to address the concerns raised in the complaint. Appeal (If Applicable): In certain cases, individuals or covered entities may have the right to appeal the OCR's findings or enforcement actions.

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.	To ensure the utmost security and privacy of our users' information, a regular review process is not currently required. Our registered users have the convenience of returning to the platform at any time to place additional product orders. To safeguard the collected data, all information is encrypted using RDS (Relational Database Service), and access is restricted solely to Privileged Users who have been approved by the System Owners. This access control mechanism ensures that only authorized personnel can interact with the encrypted data, providing an additional layer of protection to sensitive information
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	The administrators will access the PII and compile it into an XML (Extensible Markup Language) file for sharing with the Government Publishing Office (GPO) to fulfill the order.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Operating Division (OpDiv) employees and contractors requiring administrative access to the websites undergo a background check and approval process by the System Owner and the Chief Information Security Officer (CISO). Upon receiving authorization, administrators are mandated to utilize Government Furnished Equipment (GFE) and adhere to a 2-Step Verification process, involving Personal Identity Verification (PIV) and passcode authentication. These security measures are in place to ensure robust protection of the system and its sensitive data.

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.	Role-Based Access Control (RBAC): Implementing RBAC allows organization to assign specific roles to users based on their job responsibilities. Each role is associated with a predefined set of permissions, granting access only to the data and functionalities necessary for that particular role. This way, users are limited to viewing and manipulating the information required for their job functions. Data Segregation and Partitioning: Data segregation involves dividing the database or information system into logical partitions, ensuring that each user or group can only access the data relevant to their tasks. This method helps prevent unauthorized access to sensitive information. Data Encryption: Employing data encryption ensures that PII remains protected, even in the event of unauthorized access. Encryption prevents unauthorized individuals from reading or understanding the data without the appropriate decryption keys. Audit Trails and Monitoring: Implementing audit trails allows organizations to track and monitor users' actions within the system. This helps identify any unauthorized access attempts or unusual activities, enhancing security and accountability. Time-Limited Access: In some cases, granting temporary or time-limited access to PII can be beneficial. Once a user's specific task or assignment is complete, their access can be automatically revoked, reducing the risk of data exposure. Two-Factor Authentication (2FA): Implementing 2FA adds an extra layer of security by requiring users to provide two forms of authentication (e.g., password and a one-time code sent to their mobile device) before accessing PII. Contextual Access Control: Contextual access control considers the user's location, device, and other factors to determine the level of access they are granted. For example, users accessing PII from outside the organization's secure network may have restricted access.
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.	Data Classification and Sensitivity · Data Privacy Principles · Risk Awareness · Access Control and Authentication · Security Best Practices · Incident Reporting and Response · Social Media and Information Sharing · Data Handling and Disposal · Compliance with Policies and Regulations

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Ethics and Compliance Training · Information Security and Privacy Training · Cybersecurity Awareness Training · Records Management Fundamentals · Records Lifecycle · Legal and Regulatory Compliance · Records Storage and Security · Electronic Records Management (ERM) · Records Retrieval and Access · Records Disposition and Destruction
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).	In consultation with Substance Abuse and Mental Health Administration (SAMHSA) Record Management Office, and with the Contract Operating Representative (COR), for the appropriate retention and disposal schedule, Public Engagement Program (PEP) will follow National Archives and Records Administration (NARA) General Records Schedules (GRS) 3.2, Item 030 (Retention: Temporary – Destroy when business use ceases). This was also recommended by both the PEP Privacy Impact Analysis (PIA)/ Privacy Threshold Analysis (PTA) reviewer and by the SAMHSA Record Management Team. Accordingly, PII data are considered "temporary", collected and used for user identification and the creation of passwords (access), and to be destroyed when the business case is for it is over
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.	All personally identifiable information (PII) stored within the system, including temporary repositories and logs, is both physically secured and password protected. Access to PII data is strictly regulated and can only be obtained through authorized requests to the SAMHSA security team, who investigate each request and provide database server dumps upon request. The security measures implemented in this environment adhere to NIST 800-53 guidelines. Additionally, all database servers secured within the SAMHSA Amazon Web Services (AWS) cloud have comprehensive physical, technical, and environmental controls in place. Only designated Division of Technology Management (DTM) personnel with database administration and oversight responsibilities possess the necessary logical access to remotely connect to the database servers and retrieve data. Furthermore, access to the servers is restricted by network access rules, permitting connections solely from specified network IP addresses. All system logs collected are encrypted and accessible only through authorized physical requests, each of which undergoes rigorous processing by a security team representative with multiple levels of approval.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	7/3/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	7/18/2024
		SOP Days Open:	15

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	7/22/2024
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 7/22/2024 The PTA/PIA has minor comments to remove bullets as they were not 508 compliance. However, since these comments are minor and can be dealt with during the 508 process we will not reject it. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	The PTA/PIA has minor comments to remove bullets as they were not 508 compliance. However, since these comments are minor and can be dealt with during the 508 process we will not reject it.	**SAOP Review Date:**	8/2/2024
		SAOP Days Open:	11

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ SAMHSA - PEP-v2 - QTR2 - 2024 - SAMHSA2052339.pdf	206334	.pdf	7/22/2024 1:29 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 14	Data Feed Service, piafrmos	7/18/2024	As the information is provided voluntarily by the customers for order fulfillment, there is no need for additional consent to collect this information. This information is explicitly provided on our website https://www.samhsa.gov/about-us/website-policies-notices/privacy.	
PIA - 22	BLAND, CRYSTAL	7/22/2024	Please remove bullets as they're not 508 compliance.	
PIA - 21	BLAND, CRYSTAL	7/22/2024	Please remove bullets as they're not 508 compliance.	
PIA - 1	BLAND, CRYSTAL	7/22/2024	Please note that ATO Planned Date has already occurred. On the next iteration of the PTA: PTA-18A: Please remove bullets as they're not 508 compliance.	

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:	8/2/2024 3:55 PM	**History Log:**	**View History Log**