Privacy Impact Assessment (PIA): SAMHSA - CSAT OTP Extranet - QTR1 - 2023 - SAMHSA1289214

Created Date: 3/19/2025 9:05 AM Last Updated: 3/25/2025 3:19 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 - CSAT OTP Extranet - QTR1 - 2023 - SAMHSA1289214	**PIA ID:**	2887241
Name of Component:	SAMHSA - CSAT Opioid Treatment Program Extranet System	**Name of ATO Boundary:**	CSAT OTP Extranet System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	777
Submission Status:	Submitted	**Submit Date:**	3/24/2025
Next Assessment Date:	N/A	**Expiration Date:**	3/24/2028
Office:	SAMHSA	**OPDIV:**	SAMHSA
Security Categorization:	Low	**OpDiv PIA ID:**	SAMHSA1289214
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)?	Yes
4:	ATO Date or Planned ATO Date.	5/10/2022
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.	No significant changes have occurred to the system since the last PIA.
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 purpose of the system is to provide and maintain support for the OTP (Opioid Treatment Program) Extranet. This system collects information on all OTPs for the purposes of maintaining accreditation renewals every three years, tracking personnel, and processing exception requests. It also stores bi-annual reports required from approved Accreditation Bodies. There are two public websites supported to allow new OTPs and new accreditation bodies to submit a request for certification outside of the OTP Extranet system. The automated data processing Web site helps the Division of Pharmacologic Therapies (DPT) achieve its goal of processing certification of its OTPs through automated submissions and approval queues among facility, state, and federal staff, as well as supports the automated processing of provider requests for treating specific patients in a manner divergent from guidelines for Opioid therapies. The OTP Extranet greatly increases the accuracy and ease with which the CSAT SAMHSA Center for Substance Abuse Treatment) is able to monitor and facilitate OTP compliance with Federal regulations. Automated letter generation, online submission of SAMHSA's Office of Management and Budget, and identification of impending accreditation and certification expiration are among the extranet's features for helping CSAT with OTP compliance requirements. The information contained in the OTP Extranet database also supplies information that can be automatically culled into specific lists that are generated through interactions with the SAMHSA website's (MAT) Medication-Assisted Treatment page.
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.	Data stored within the system includes emails, names, phone numbers and addresses of system users and opioid treatment programs. Users are removed from the system at the request of SAMHSA. Other data includes letters, certifications, and other information on opioid treatment programs.
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 Email Address

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.	All information collected and maintained in the system, including PII, is for the purpose of helping the Division of Pharmacologic Therapies (DPT): a) achieve its goal of processing certification of its OTPs through automated submissions and approvals, as well as, b) for the purpose of supporting the automated processing of provider requests for treating specific patients in a manner divergent from guidelines for Opioid therapies
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)?	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 purpose of the system is to provide and maintain support for DPT's role in monitoring opioid treatment programs. SAMHSA/DPT personnel, State Opioid Treatment authority personnel, OTP personnel, and Accreditation Body personnel have access to the system. Public URLs provide user log in via email and password.
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?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
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.	Web bug/beacons - 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 Mailing Address Medical Records Number Patient ID Number Other - Free text Field - medical notes (i.e., without patient identifying information), and information reflecting aspects of the patient's treatment plan (i.e., schedule, drug and dosage, reasons for exception request being filed).
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 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.	Above 2000

PIA - 4:	For what primary purpose is the PII used?	For the purposes of establishing, verifying, and maintaining an Opioid Treatment Program (OTP) Extranet user account, the system collects names, e-mail addresses, phone numbers, and mailing addresses on system users/account-holders (i.e., OTP personnel, Substance Abuse and Mental Health Administration (SAMHSA) staff, State Opioid Treatment Authorities (SOTAs), or contractors with responsibility for maintaining the OTP Extranet system). The names and contact info of SOTAs are also used to create real-time lists of SOTAs that can be accessed from links on the SAMHSA website. Names and contact information of responsible organizational officials from applicant accreditation bodies, and names and contact information of signatories of patient exception requests and applications for certification to use opioid drugs in a treatment program, are used to track and process the respective forms. SAMHSA and SOTAs use the following information from the Exception Request and Record of Justification Exception (SMA-168 form) to assess the merits of the patient exception request and derive a final approval/denial: patient Identification (ID), medical notes (i.e., without patient identifying information), and information reflecting aspects of the patient's treatment plan (i.e., schedule, drug and dosage, reasons for exception request being filed). SAMHSA uses the OTP-assigned patient Identification (ID) to track the patient exception requests (SMA-168) submitted for approval by a given OTP, while the other Personally Identifiable Information (PII) information from the SMA-168 provides necessary information used by state opioid treatment authorities, and SAMHSA/CSAT (Center for substance Abuse Treatment) to approve or deny a physician's request to treat a specific patient in a manner divergent from guidelines for opioid therapies.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Program monitoring as related to questions of interest that SAMHSA might have about the number and nature of patient exception requests filed in a given timespan, and characteristics of facilities that use the OTP Extranet to file them.
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 OTP Extranet system supports SAMHSA's information collection requirements established for opioid treatment programs (OTPs) in regulations contained in Title 42 of the Code of Federal Regulations (CFR) Part 8, by establishing electronic data submission and processing/approvals of two data collection forms used to implement the regulations (Office of Management and Budget (OMB) No. 0930-0206): SAMHSA (or "SMA") forms SMA-162 and SMA-168. To become certified, an OTP must be accredited by a SAMHSA-approved accreditation body and must comply with any other conditions for certification established by SAMHSA. The regulations were promulgated under authority of Section 4 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (P. L. 91-513) and Section 303(g) of the Controlled Substances Act (CSA) (21 U.S.C. 823(g)(1)), as amended by the Narcotic Addict Treatment Act (NATA) (P. L. 93-281). SAMHSA has statutory authority for this program under Sections 501(d)(5) and (7) of the Public Health Service Act (42 U.S.C. 290aa). OTPs are governed by 42 CFR Part 2, "Confidentiality of Alcohol and Drug Abuse Patient Records" as a condition of their certification by SAMHSA, and all users of the system attest to their adherence to 42 CFR Part 2 at the time of requesting their account. The regulations established under 42 CFR Parts 8.3, 8.4, and 8.6 establish requirements for OTP accrediting bodies.
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, First Name and Last Name
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.	https://www.federalregister.gov/documents/2010/05/20/2010-12147/privacy-act-of-1974-report-of-systems-of-record-notices Opioid Treatment Waiver Notification System (OTWNS) 09-30-0052 1
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV State/Local/Tribal
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	SMA-162 & SMA-168 – OMB Number 0930-0206
PIA - 10B:	Identify the OMB information collection approval number expiration date.	9/27/2027
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?	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" from users providing their name and contact information-- if they want an OTP Extranet account, they must supply their information as a requirement of SAMHSA's procedures for verifying the identity of accountholders to ensure only authorized and appropriate users have access to the system. With respect to PII associated with patient exception requests, there is also no "opt out" provided for the PII because this is (1) necessary information needed by the OTP program, per regulatory requirements that they must keep patient records, (2) required for SAMHSA to track and approve/deny the request, and (3) regulations dictate that the activities associated with audit and evaluation activities do not require patient consent. The specific process by which patients are provided this disclosure is specific to each of the nation's 2100+ OTPs but it generally occurs at time of admission to treatment when they receive a written summary of conditions related to treatment consent
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.	Users of the OTP Extranet system consent at the time of obtaining their account to their data being monitored, recorded and subject to audit. With respect to patient data/ PII, patients are informed through patient consent procedures at the time of admission to treatment (or as soon after as is clinically feasible) that the OTP's patient data is subject to sharing without patient consent for audit and evaluation purposes as governed by regulation. This is part of a process that happens in a manner and time specific to intake/admission/ treatment consent processes at each of nation's 1700+ OTPs.

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.	As a condition of applying for an account, users attest that if they become aware of unauthorized attempts to gain access to their account or of unauthorized or inappropriate use of the system, they will contact the OTP Extranet Information Center staff at otp-help@jbsinternational.com or call the Support phone number, who will work with the OTP Extranet developer, SAMHSA, and program director to investigate the concern and, if appropriate, disable the account. Names and contact information of accountholders are kept current through regular use of the system. Passwords must be updated every 60 days, which requires users to go to their profile page that also displays their contact information. Discrepancies noted by users can be resolved by contacting the OTP Extranet Information Center staff at otp-help@jbsinternational.com or call the Support phone number. Accounts unused for 60 days are administratively deactivated. With respect to the medical record number (i.e., the OTP-specific patient ID), treatment plan info, and medical notes information that may be contained in the data obtained from SMA-168 forms (i.e., the other PII items listed in question 15), according to regulatory guidance about patient alcohol and drug treatment records, the identifying patient number (patient ID) is not considered to be patient-identifying information if it does not consist of or contain Social Security Number (SSN), driver's license or other numbers that can be used to identify a patient with reasonable accuracy and speed from sources external to the program. Only the OTP facility holds the key to the identity of the person to whom the patient ID is coded. Thus, information provided by OTP program staff through the OTP Extranet system is not considered to be personally identifying, per the regulatory specification that the ID is not PII; nor is it easily linkable back to the patient's actual identity. Processes and guidelines surrounding disclosures of patient data sit outside of the OTP Extranet system are governed by regulatory compliance rules between SAMHSA and OTPs. Further, for patients to be granted take-home medication, the physician treating them has to submit the SMA-168 that contains some patient information in order to get the State's and SAMHSA's approval. It is part of the individual's treatment plan and, by law, the only way to be granted approval to take-home medication that is a Schedule II controlled substance. Review of the treatment plan happens between the patient and physician/OTP. Thus, agreement on the course of treatment that would include the request for, or change in, take-home medication, happens outside of the OTP Extranet system that collects the outcome of that decision in the form of a physician-signed SMA-168 request for exception.

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.	With respect to patient information listed in this system as "PII" (i.e., medical record number, medical notes, manually entered items), this data is entered into the SMA-168 form and signed by a treating physician; after that the data is read-only. SAMHSA staff is allowed to view the form data, but not to modify it. It is archived after one week and no longer accessible through the system. Our one-week review is the extent of the access and there is no additional process in place at this time.
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 have access to their own PII (names, contact information) because they, themselves, provide it into the system when applying for an account. Certain types of users also have access to the names and contact info of other users since program directors, SAMHSA, and contractors are involved in verifying user accounts. Program directors manage (approve/deny account requests; can deactivate accounts) of OTP Extranet users in their own program. Thus, access to any PII that is related to obtaining/verifying/ maintaining user accounts is accessible by appropriate permissions solely for administrative purposes. There are nine contractor/developers from the JBS International, Inc. team who have rights to all system information to monitor the system and resolve issues and questions from users. Developers are assigned contractors that are information center staff who provide internal technical assistance during development. Contractors are the developers and information center staff who need access to the PII to be able to solve problems that arise with the data, form, or electronic approval process; or with establishing/verifying an account. PII listed in question 15 from the SMA-168 form (e.g., patient ID/medical record number and medical notes) may be needed by contractors to fulfill ad hoc analytic requests from SAMHSA regarding the filing of patient exception requests and who/why those requests are being filed. This is solely for program monitoring purposes/ program evaluation.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The system uses the user authentication where only users that have approved roles are allowed to view the 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.	The roles, permissions, and restrictions are strictly defined in the system. Names and contact info required to establish, verify, and monitor a user account is viewable by nine people from the JBS team holding an Admin role (five JBS contractor/developer staff and four staff from the OTP Extranet Information Center) and SAMHSA compliance officers. Additionally, a specific user from each OTP holding a program director role has access to this information for all users from his or her OTP. Program directors have authority to approve, deny, and deactivate user accounts from their assigned OTPs. In regards to the information from SMA-168 that is classified in question 15 as PII (i.e., the patient id, medical notes, other info that gets checked off related to drug/dosage, schedule, employment status, etc.), the information is viewable by all OTP Extranet users from the OTP for which the SMA-168 is filed (i.e., all four OTP user account types--Program Director, Program Sponsor, Program Physicians, and Counselor account-holders), as well as SAMHSA users, SOTAs, and the nine Admin users.
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.	Developers and contractor staff, including OTP Extranet Information Center (i.e., help desk) staff, have appropriate trainings annually in Health and Humana Services (HHS) information security and privacy. All current information center staff and JBS staff working on the project and interacting with its data have certificates of completion on file for the HHS records management training. Additionally, JBS staff have annual trainings in general on IT security issues (e.g., security awareness and handling sensitive information).
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users employed by an OTP have any of four different account types/ permissions levels, as appropriate to their role in the program (i.e., program counselor [a non-physician staff member not permitted to sign SMA-168 requests]), program physician (i.e., the only role allowed to sign SMA-168 forms), program sponsor (i.e., the only role allowed to authorize various changes to the program structure); and program director. A series of trainings, one specific to each role, was provided. Manuals as well as training information are available from SAMHSA (one for each of the four OTP user role types) describing the OTP Extranet account features.

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 National Archives and Records Administration's (NARA's) General Records Schedule (GRS) 3.2 Transmittal 33 is currently being used as records management (RM) schedule. No records are removed from the database [retention period indefinite]. Records that are older than 1 week are archived and are no longer available through the system. Hard copy media will be destroyed. A crosscut or diamond cut shredder shall be used to ensure proper destruction beyond reconstruction/recognition. All Information Technology (IT)- managed storage hardware designated for disposal (e.g., hard drives, printers, magnetic media) is physically destroyed by JBS's recycling vendor by shredding the hardware to guarantee 100% destruction of all data. Smaller bulk sensitive optical media (e.g., "Compact Disc/ Digital Video Disc (CD/DVD)) can also be physically destroyed via document cross-cut shredding devices. SAMHSA will be following the records retention policy of its cloud services
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.	The contractor, JBS, is developing and maintaining the software and employs a proper blend of administrative, technical, and physical controls that are fully described in the OTP Extranet's system security plan (SSP) document. Specific controls related to the protection of PII collected for OTP Extranet web application include administrative controls, i.e., policies that require the application of least privilege model on technical and physical controls; technical controls, i.e., operating system and database account management, operating system folder permissions, database access controls, use of two-factor authentication for administrator access to database server desktop (IT system administrator access), strong password standards, account expiration, and account lockout for both web application and Windows operating system, next generation firewall; and physical controls, i.e., physical safeguards that include proximity badge access to data center, IT area, and building, video surveillance and visitor control to data center.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	3/24/2025
Privacy Analyst Comments:	PTA 12A: Unable to edit PTA Responses, see below for updated and correct response Session Cookies- Collect PII Persistent Cookies- Does not Collect PII	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	12 A is verified correct by the system owner.	**SOP Review Date:**	3/25/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/25/2025
Agency Privacy Analyst Review Comments:	All previous comments regarding the PIA has been addressed.	**Agency Privacy Analyst Days Open:**	0

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	3/25/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 4	Data Feed Service, piafrmos_Release	3/19/2025	Refer to PIA 15 and 16 for clarification and explanation of "other PII" mentioned for second form.	
PIA - 8B	VILLAFUERTE, NESTOR	3/19/2025	Reviewer notes that https://www.samhsa.gov/system-notice-09-30-0052-1 leads to a page that does no longer exist. Please update.	
PIA - 1	BLAND, CRYSTAL	3/20/2025	PTA-12A was the response in error "web bug/web beacons-collect PII?"	
PIA - 1	BLAND, CRYSTAL	3/20/2025	Per PIA-4, PTA-5, PIA-16 and PIA-1 need to add the following PII elements to their responses "patient identification (ID), medical record number, medical notes (i.e. without patient identifying information), and patient's treatment plan."	
PIA - 23	BLAND, CRYSTAL	3/20/2025	Per https://www.archives.gov/records-mgmt/grs.html, please update to reflect the most current General Record Schedule which is 3.2 transmittal 33.	
PIA - 8B	BLAND, CRYSTAL	3/20/2025	Please update the URL to the SORN to https://www.hhs.gov/foia/privacy/sorns/samhsa-sorns.html or you can use the federal register URL https://www.federalregister.gov/documents/2010/05/20/2010-12147/privacy-act-of-1974-report-of-systems-of-record-notices.	

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:	3/25/2025 3:19 PM	**History Log:**	View History Log