Privacy Impact Assessment (PIA): FDA - IAM - QTR1 - 2025 - FDA4901286

Created Date: 1/31/2025 3:41 PM Last Updated: 2/20/2025 12:37 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:	FDA - IAM - QTR1 - 2025 - FDA4901286	**PIA ID:**	2726140
Name of Component:	FDA - CTP Industry Account Manager (IAM) Portal	**Name of ATO Boundary:**	CTP Electronic Submissions
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	20
Submission Status:	Submitted	**Submit Date:**	2/10/2025
Next Assessment Date:	02/20/2028	**Expiration Date:**	2/20/2028
Office:		**OPDIV:**	FDA
Security Categorization:	Moderate	**OpDiv PIA ID:**	FDA4901286
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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	9/9/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred 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 Center for Tobacco Products (CTP) Electronic Submissions system (eSub) is a suite of database-supported applications that facilitates the collection, logging, tracking, and retrieval of documents provided to the Food & Drug Administration (FDA) by the tobacco industry and others (e.g., adverse experience reports from the general public). CTP uses this data to evaluate tobacco products, develop policy, and assess industry compliance with the Family Smoking Prevention and Tobacco Control Act (FSPTCA). The eSubmissions suite is comprised of several applications/components which are covered in their own respective Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA). This PTA/PIA will focus on the Industry Account Manager (IAM) Portal component. Industry Account Manager (IAM) Portal component is part of the FDA's CTP Office of science program. The public facing website, hosted on the FDA Internet, accepts IAM requests submitted by the Tobacco industry representatives. IAM users have the option of submitting their request via electronic submission through the website. The CTP IAM Request System collects information from organizations that need to establish a CTP Portal account. The FDA reviews IAM account requests and establishes the IAM CTP Portal account. The Industry Account Manager (IAM) is an individual designated by the authorized representative of an organization and acts as an administrator (“admin”) for the organization’s CTP Portal Next Generation user accounts. Once the IAM account is created by CTP, the IAM is given an “admin” role, and can create, manage, and set roles for all of the organization’s employees’ CTP Portal Next Generation user accounts*, including user accounts for non-employee attorneys or agents. The selected IAM will manage CTP Portal user accounts for the listed organization. Account management will include establishing and deactivating user accounts based on individual need for CTP Portal access. The IAM may create accounts for an external attorney or other agent. If an attorney or agent no longer represents an organization, the IAM for the associated organization is responsible for deactivating that person’s CTP Portal user account to prevent further access.

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 CTP IAM Request System collects descriptive information regarding the individual authorized to request the CTP IAM account and the individual designated the IAM for the requesting organization. FDA systems will assign an IAM account to each approved request and provide that account identifier, username and password to the requestor and the individual designated as the IAM.
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 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 CTP IAM Request System decreases the burden and increases the efficiency related to the preparation of CTP IAM requests and Office of Science (OS) review of those requests. OS staff do not use any personal identifiers to retrieve records held in the CTP IAM Request System. Retrieval is based on organization name. Information collected relative to individuals includes name, job title, and contact information including e-mail address, telephone number, mailing address, and electronic signature.
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.	To access the CTP Portal for regulatory submissions, Industry will need to request a designee to establish their first CTP Portal user account via the public facing IAM website. This individual will be the organization's primary Industry Account Manager (IAM). Once the CTP Portal account and IAM user account are created, the IAM will manage all the CTP Portal user accounts for your organization. Public users access the website via public URL (https://www.accessdata.fda.gov/scripts/IAM/).
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.	Session Cookies - Does Not Collect PII Persistent 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?	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 User Credentials Other - Free text Field - organization name, job title, account identifier, and electronic signature.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000

PIA - 4:	For what primary purpose is the PII used?	The CTP IAM Request System collects information that is used by the OS to authorize establishment of an IAM account for the requesting organization. The IAM is responsible for establishing and managing user accounts that are subsequently used to manage CTP portal access privileges.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The FDA makes no secondary use of the PII.
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.	21 U.S.C. 301, sections 375(b), 387d, and 387e of the Federal Food, Drug, and Cosmetic Act, as amended by the Family Smoking Prevention and Tobacco Control Act (Pub. L. 111-31, 123 Stat. 1776), incorporated at 18.U.S.C. 1001, Section 910.
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.	0910-0879
PIA - 10B:	Identify the OMB information collection approval number expiration date.	12/31/2028
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.	An individual must provide their PII in order to have an IAM account. Failure to provide this information means that the individual would be unable to serve as an IAM.

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.	Individuals whose PII is in the system will be notified of a major change by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice, or informal processes such as email notice to the individuals.
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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA and CTP system have several avenues available to resolve the situation using contact and reporting information available across FDA.gov including contacting or submitting concerns to the FDA Privacy Office. Employees aware of potential unauthorized use of PII in the system may submit concerns to their supervisor, the FDA Privacy Office, a 24-hour technical assistance line, and FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC).
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.	Users ensure data integrity and accuracy when they create a portal account and enter their information. Availability is ensured by the portal giving access to account holders. Relevancy is ensured by only requiring information needed to create a portal account.
PIA - 17:	Identify who will have access to the PII in the system.	Users 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: Designated CTP staff require access to review and authorize creation of an IAM accounts. Developers: For system development and upkeep and for trouble shooting issues related to the system, performance and access. Contractors: CTP uses Direct Contractors for system development and upkeep. They trouble shoot issues with system, performance, and access. No PII collected for Contractor, Direct Contractors do not analyze the data that is collected.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA Privacy and security practices require that individuals should only be granted PII access privileges necessary to do their job. These policies are required under the Federal Information Security Modernization Act (FISMA) and are documented in FDA Information System Security Plans. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.

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.	A Standard Operating Procedure (SOP) and System Access Request (SAR) form is used to grant different levels of system access based on work need and role. The relevant supervisor will indicate on the eSubmissions user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria. All users are authenticated.
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.	All system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Digital Transformation (ODT) verifies that training has been successfully completed and maintains a record of certificates of training on all FDA employees and Direct Contractors.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Personnel are trained on the use of the system and review the HHS/FDA Rules of Behavior. Additional role-based training on privacy is available via FDA's Privacy Office.
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 electronic data captured by eSubmissions is currently retained indefinitely, pending receipt of the requested FDA file code consistent with the National Archives and Records Administration (NARA) guidelines. The selection of this retention schedule is under review and will be updated as necessary. CTP anticipates that the file code will be FDA's file code 6132, consistent with NARA-approved schedule N1-88-07-2, for Adverse Experience Reporting System Database Records, for which record retention are cutoff annually at the end of the calendar year after a case is closed and deleted 30 years after cutoff or when no longer needed for trend analysis or reference purposes, whichever is the latest.

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 safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/10/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**SOP Review Date:**	2/10/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/11/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 2/11/2025 All comments addressed, this PIA is ready for SAOP review and approval. 2/7/2025 Please see comments and update accordingly: Updates for the PTA (next iteration): PTA-5: Please list the PII elements being collected: Name, job title, contact information (i.e. email, phone number, mailing address,), organization name, account Identifier, user credentials (i.e. username and password), and electronic signature." PTA-11 should be marked "No" in the next iteration of the PTA as it contains links to social media sites such as Twitter and Facebook. PIA-1: Please add e-mail address, and mailing address and check "other- organization name, job title, account identifier, and electronic signature."	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Updates for the PTA (next iteration): PTA-5: Please list the PII elements being collected: Name, job title, contact information (i.e. email, phone number, mailing address,), organization name, account Identifier, user credentials (i.e. username and password), and electronic signature." PTA-11 should be marked "No" in the next iteration of the PTA as it contains links to social media sites such as Twitter and Facebook. PIA-1: Please add e-mail address, and mailing address and check "other- organization name, job title, account identifier, and electronic signature."	**SAOP Review Date:**	2/20/2025
		SAOP Days Open:	9

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
1-31-2025 EMAIL_PIA in Queue (CTP Industry Account Manager (IAM) Portal).pdf	393738	.pdf	2/5/2025 7:51 AM	0
CTP Industry Account Manager (IAM) Portal_SOP Approved.pdf	161950	.pdf	2/5/2025 7:51 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	2/7/2025	Per FDA's Email: The PIA is experiencing an Archer error with Question #3 of the general information. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” The FDA instance of Archer is automatically entering the answer “*No*,” which is incorrect. The ATO date is 9/9/2022. *At this time, we are unable to update Archer to reflect the correct answer “Yes.”* The FDA Archer Team is aware of the occurrence and is working on a solution.	
PIA - 1	VILLAFUERTE, NESTOR	2/7/2025	Reviewer notes that PTA-11 should be marked "No" in the next iteration of the PTA as it contains links to social media sites such as Twitter and Facebook. PIA-1: Please add e-mail address, and mailing address as they are listed as PII elements in the PTA.	
PIA - 1	BLAND, CRYSTAL	2/7/2025	PTA-5: Please list the PII elements being collected: Name, job title, contact information (i.e. email, phone number, mailing address,), organization name, account Identifier, user credentials (i.e. username and password), and electronic signature." PIA-1: In addition to Nestor comment please check "other- organization name, job title, account identifier, and electronic signature.	

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:	2/20/2025 12:37 PM	**History Log:**	View History Log