Privacy Impact Assessment (PIA): - QTR1 - 2024 - FDA2125157

Created Date: 1/30/2024 3:06 PM Last Updated: 12/2/2025 4:25 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:	- QTR1 - 2024 - FDA2125157	**PIA ID:**	1761481
Name of Component:		**Name of ATO Boundary:**	
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	62
Submission Status:	Submitted	**Submit Date:**	1/30/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2125157
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	1/12/2024
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.	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 subject of this assessment is the FDA Center for Devices and Radiological Health (CDRH) Office of Science and Engineering Laboratories (OSEL) Regulatory Science Tools - Catalog component ("RST-Catalog" or "RST-C" or "the system") within the CDRH Scientific and Research General Support systems (boundary). FDA's Office of Science and Engineering Laboratories (OSEL) uses RST-Catalog to provide a public facing website for hosting developed regulatory science code, tools, models, applications, datasets, lab methods, documentation, and similar materials. This RST-Catalog website enables general public and industry to access, run, and/or download content controlled by OSEL. RST-C advances the FDA's ability to support OSEL as well as rapidly develop and distribute pre- and post- market scientific evidence related to the safety, effectiveness and quality of medical devices subject to FDA approval and regulation.
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 types of information collected into, maintained and/or shared via the system are: 1) internal administrative user account information consisting of personally identifiable information (PII) in the form of name, username, email address (all PII about FDA personnel and direct contactors; no external users information is collected); and 2) regulatory science code, and information about tools, models, applications, datasets, lab methods, documentation, and similar materials related to CDRH-regulated products . System users consist of Administrators and Content Editors. Note that user access credentials (to verify identity and control access to RST-C) are maintained in a separate system (e.g., Active Directory (AD), AMS) and not collected or maintained by this system. CDRH maintains the PII in the system from use account creation until the account is no longer needed and is deleted.
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.	

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 about regulatory science code, and information about tools, models, applications, datasets, lab methods, documentation, and similar materials is collected, maintained and/or shared via the system for the purpose of …disseminating to the industry or public. The information about RST-C users (FDA employees and direct contractors) is collected and /or maintained to authenticate user identity and control access to RST-C by means of username and/or email address. Collection of the user's name is collected for human recognition to associate an individual with their email or username and subsequently, identification of the account to the individual. The RST-C webpage provides search functions so members of the public may find and access publicly available information maintained by the FDA.
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 RST Catalog is a public facing website hosting OSEL's regulatory science code, tools, models, applications, datasets, lab methods, documentation, and similar materials. The RST-Catalog website enables external stakeholders to access, run, and/or download content controlled by OSEL. RST-C supports CDRH efforts to rapidly develop and distribute pre- and post- market scientific evidence related to device safety, effectiveness, and quality. The following categories of individuals have access to the website: authenticated administrators, content editors and unauthenticated members of general public. These users can access the homepage and access the backend via SAML/login. Whereas general public users access the website via Homepage and cannot access the backend of the website. The system/webpage administrator and editors access the website via public facing pages requiring authentication, while unauthenticated users (general public) access the website via public facing pages. Note that the specific URL has not been established as of the time of this assessment.
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.	
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?	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 User Credentials Other - Free text Field - User credentials consists of username and password.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Below 50
PIA - 4:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of user authentication.

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.	5 U.S.C. 301
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 Other Government Sources Within the OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	The system does not collect any information on the public and therefore, does not require an OMB information collection approval number.
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.	FDA users provide their contact information as a practical requirement in order to gain access to the system. There are no opt-out procedures specific to OSEL RST Catalog.

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.	The OSEL RST Catalog does not anticipate major changes to the type of PII ingested/maintained in the system or in how it is used. Should such a situation arise, the team will notify system users of the change and as needed obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.
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 the system contains incorrect contact information for a user, the account likely will not function correctly and system administrators would fix the issue. If a user notices incorrect information in their account, the user can contact system administrators to fix it. Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone, and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel must report that without delay to the 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.	Accuracy of PII is ensured during periodic user account maintenance and during the user onboarding/offboarding process. Relevancy is ensured by the design of the system which limits the type of PII collected to PII necessary for individual identity verification. Applied access settings and other security controls support PII integrity, availability and accuracy. Maintenance of cameras, scanners, servers and applications provide additional security.
PIA - 17:	Identify who will have access to the PII in the system.	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.	Administrators, Developers and Contractors: identify and manage user access.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. 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.	System administrators require access to account information in order to manage and maintain the system. There is minimal PII contained in OSEL RST Catalog. The relevant supervisor will indicate on the 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 using technical controls and system settings.
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 Information Management and Technology (OIMT) verifies that individuals successfully complete the training.
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 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).	In regard to the retention and destruction of PII, due to it pertaining to the identification of a user account, it is retained for the same duration the account is active and destroyed when the account is no longer active. Specifically, records are maintained under FDA File Code FDA-9962 and NARA Approved Citation GRS 3.2 Item 030 (System access records; Systems not requiring special accountability for access). Disposition: TEMPORARY. Destroy when business use ceases.

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:**	1/30/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	1/30/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/1/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski This PIA is ready for SAOP review and approval. Also please note in the General Information section the Name of Component and Name of ATO Boundary info as well as part of the PIA name is missing. The exported version of the PIA is attached in Supporting Documentation.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Also please note in the General Information section the Name of Component and Name of ATO Boundary info as well as part of the PIA name is missing. The exported version of the PIA is attached in Supporting Documentation.	**SAOP Review Date:**	3/12/2024
		SAOP Days Open:	40

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CDRH Office of Science and Engineering Laboratories RST - Catalog_SOP Approved.pdf	171670	.pdf	2/1/2024 8:59 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 9	Data Feed Service, piafrmihs	1/10/2024	Other: Internal via Ping Federate SSO	
PIA - 1	BLAND, CRYSTAL	2/1/2024	Update on the next iteration of the PTA: PTA-5: States that user credentials are maintained by another system, please include in your response that the system is covered in a separate PIA. PTA-5A: Per PTA-5, user credentials are maintain by another system so the response for PTA-5A should have been "Yes, but maintained by another system..." Also please note in the General Information section the Name of Component and Name of ATO Boundary info is missing.	

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:	12/2/2025 4:25 PM	**History Log:**	View History Log