Privacy Impact Assessment (PIA): FDA - ROMS - QTR1 - 2025 - FDA4900702

Created Date: 1/10/2025 7:24 PM Last Updated: 1/30/2025 1:15 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 - ROMS - QTR1 - 2025 - FDA4900702	**PIA ID:**	2628959
Name of Component:	FDA - OII Regulatory Operations Management System	**Name of ATO Boundary:**	OII Case and Workload Management
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	20
Submission Status:	Submitted	**Submit Date:**	1/10/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/30/2028
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4900702
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)?	No
4:	ATO Date or Planned ATO Date.	
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 initial release will include a subcomponent called Field Accomplishment Services (FAS), the part of the Atomic Regulatory Process framework in which key operations will leverage: Domestic Sample Collections Domestic Field Exams Recall Audit Checks (RACs) US Food and Drug Administration (FDA) personnel located at headquarters, in the field offices, and various FDA centers and lab locations utilize these tools to support the inspections, investigations, recalls, and other related compliance and enforcement activities required for effective support of the FDA mission and the safety of the public. The relationship of this system to other FDA systems is that Regulatory Operations Management System (ROMS) will integrate within the Office of Inspections and Investigations (OII) systems, data entered into Field Accomplishments and Compliance Tracking System (FACTS) and Assignment Management Services (AMS) system and stored in the Operations Database. Import data stored in the Operations database can be synced with ROMS to allow for users to enter data relating to Sample collection, fields examination, and Recall Audit Checks. The users of the ROMS system will be FDA personnel. ROMS is configured to use Single Sign On (SSO), and it allows the FDA personnel to log in with their personal identity verification (PIV) cards.

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 the system include FDA employee details including first and last name, email, and role. Sample and field exam details including Product, PAC, Location, Descriptions\labels, method of storage, payment details, and the collector details (FDA personnel assigned to collection). RAC functionality gathers the above details in addition to details for FORM 3177 including consignee (firm name, address, contact number, and disposition information). The types of data that are maintained in and/or shared from the system is/are professional contact information. The primary functions of ROMS include the collection, maintenance and sharing of several types of data. For workload management, the PII used includes: assignment requester first and last name, FDA point of contact (POC) first and last name, POC work/FDA phone and fax numbers. Non-PII used for workload management includes: FDA assignment organization, assignment date, assignment subject, assignment status, FDA operations, review remarks, products reviewed/sample collected. For Field operations, the PII used includes: FDA inspector first and last name as well as Direct Contractor state inspector first and last name. The non-PII used in inspections and field operations includes: inspections results, processes/conclusions, division decisions, product description, investigation reason, findings and recommendations, adverse inspectional observations, inspection summary, products covered/description, inspection refusals, and operation remarks. For sample collections, the PII employed includes: FDA sample collector first and last name. Non-PII used in this context includes: sample description, collection reason and remarks, firm FEI and firm name, firm type, product name and description. FDA employees and Direct Contractors (system users) request a user account for ROMS and provide PII data including their first name, last name, work phone, work fax, work email and work address along with their internal employee number (used for identification in the Enterprise Administrative Support Environment (EASE), an FDA system with its own PIA).
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is
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 FDA employees and contractors is collected and/or maintained in order to facilitate workload management and tracking of completed work. The information about consignees and firm details is collected and/or maintained in order to allow for tracking of field exams, sample collections, and recall audit checks. PII from the system/component/collection is shared internally within the FDA only in order to facilitate any reporting compliance requirements as necessary.
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)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	ROMS, a web-based application, provides modern technical functionality to streamline field operation tasks performed by investigative and supervisory staff. The life cycle of a field operation encompasses initiation, assignment, execution, data collection, and endorsement of findings. Key functionality of ROMS: Enabling supervisors to assign work to investigators · Allowing investigators to manage their field operation workloads · Facilitating research about each operation · Executing specific tasks and collecting relevant data, documentation, and evidence · Developing and submitting reports for supervisory review · Enabling supervisors to review, return for rework, or endorse operations · Facilitating decision-making on any required next steps The users of ROMS will be FDA employees and contractor administrators. They will log into the website via Single Sign On (SSO) which interfaces with Active Directory. In order to gain access to ROMS, you will need the appropriate roles set in the database that limit a users access based on their position.
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?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Phone numbers User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors 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?	The FDA uses the PII in Regulatory Operations Management System (ROMS) to manage the process of reviewing applications for FDA approval of drugs, devices, cosmetics, and other FDA-approved items; manage federal/state partnerships; manage workloads and analyze activity metrics; conduct investigations and compliance reviews; and to contact individuals employed by regulated businesses and organizations. Business contact information for FDA personnel and industry points of contact, are collected for communicating with firms in relation to recall activities, and the tracking and managing of the FDA's processing and administration of the activity. The PII is used to accurately document an inspection for compliance, for business contact purposes, and in support of enforcement and analysis activities where inspection data is relevant.
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.	Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 374; Public Health Service Act, 42 U.S.C. 262-264.
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 In-person Government Sources Within the OPDIV Non-Government Sources Members of the Public
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.	This does not fall under the definition of an information collection request as defined by the Paperwork Reduction Act (PRA).
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.	State or Local Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	The PII is shared and disclosed with State partners to assist with contracted inspections.
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)).	N/A
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.	All PII is given voluntarily and gathered under the authority of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 374; Public Health Service Act, 42 U.S.C. 262-264 as part of a regulated inspection or investigation. Before PII can be shared, non-disclosure agreements, memorandum of understanding, and information sharing agreements must be documented.
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.	Establishment personnel provide PII voluntarily. They may object or discuss inspection observations with the FDA representative during the inspection or by contacting the FDA after the inspection. FDA personnel are required to provide their name and work contact information in order to get authorization to access the system.
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.	If FDA practices change with regard to the collection or use of PII in the System for Inspections, Recalls, Compliance, and Enforcement (SIRCE), the agency will provide any required notice and obtain consent from individuals. Notice procedures may include Federal Register notices, hard copy mail to individuals, adding or updating online notices and disclaimers, or using other available technological means for notification and consent.

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.	Personnel may raise concerns and/or submit data corrections through supervisory channels and FDA's Employee Resource and Information Center (ERIC). Individuals who are members of the inspected establishment may contact FDA through numerous email, phone and standard mail avenues (all listed on fda.gov). Additionally, there is a review process during the inspection that allows for a firm point of contact to review the final inspection reports and identify anything that they feel is inaccurate. 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.	All PII is relevant because point of contact information is necessary to communicate with regulated establishments. PII (name and work contact data) is provided by the establishment or the individual establishment employee, and the individual and/or establishment is responsible for providing accurate information. Accuracy is ensured by individual review of inspection reports and correcting data in the course of OII's use of the system/information, e.g., updating name and phone number for entity point of contact. Firms/individuals may amend their submitted contact information by contacting FDA. FDA personnel may correct/update their information themselves. Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls are selected based on NIST guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. OII performs regular reviews to ensure that the information provided is correct.
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?	No
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Performing and documenting FDA Inspections. Administrators: Administrators have access to PII in the course of performing analysis of historical activities and to review work in process. Developers: Developers have access to PII to perform level 3 helpdesk support Contractors: Helpdesk direct contractors have access to PII to perform level 1 and 2 helpdesk support activities.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System access requests are reviewed and approved by the system/business owner along with the SIRCE management team. System accounts are reviewed on a regularly basis to determine if access is still required for each user. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access).
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.	Supervisors indicate when accounts are created to apply the minimum information system access that is required for the user to complete his/her job. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
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 FDA personnel complete mandatory security and privacy awareness training at a minimum of once a year, including annual Computer Security Awareness Training (CSAT). This training includes 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.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System users receive system-specific training, review the HHS 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 records handled in ROMS are governed by a variety of records schedules specific to the nature of the records. The retention and destruction periods generally range from 10 to 30 years after an action closes or when a record is no longer needed. ROMS database records are maintained in accordance with National Archives and Records Administration (NARA) approved citation N1-088-09-3 which states that records disposition is temporary, with records deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final. Program management files fall under NARA approved citation N1-88-07-2.
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 uses of firewalls; access controls such as user names and passwords; and regular testing of information technology systems. Physical controls include that all system servers are located at FDA 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:**	1/10/2025
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:**	1/10/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	1/17/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 1/17/2025 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	7

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	1/30/2025
		SAOP Days Open:	13

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
OII Regulatory Operations Management System_SOP approved 1.20.2025.pdf	172628	.pdf	1/13/2025 8:58 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Admin Section

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

Miscellaneous Fields

Last Updated:	1/30/2025 1:15 PM	**History Log:**	View History Log