Privacy Impact Assessment (PIA): FDA - LIMS - QTR4 - 2024 - FDA4899082

Created Date: 11/27/2024 11:25 AM Last Updated: 12/4/2024 2:20 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 - LIMS - QTR4 - 2024 - FDA4899082	**PIA ID:**	2486992
Name of Component:	FDA - OII Laboratory Information Management System	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	8
Submission Status:	Submitted	**Submit Date:**	11/27/2024
Next Assessment Date:	N/A	**Expiration Date:**	12/4/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4899082
Legacy PIA ID:		**Make PIA available to Public?:**	No

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.	10/20/2022
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The Laboratory Information Management System (LIMS) now collects personally identifiable information (PII) and has undergone minor changes to address defects and minor enhancements to the Inventory, Material and Equipment Management modules. FDA has decommissioned the sample management module that was part of the system.
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 Laboratory Information Management System (LIMS) in this context is the Commercially-Available Off-The-Shelf (COTS) software (vendor name is StarLIMS) and custom software that directly supports the FDA's Office of Regulatory Affairs (ORA) Laboratory Management Program. LIMS foundational modules (inventory, media, material, suppliers and equipment management) are implemented in the ORA laboratories. The inventory and media modules are foundational modules that allow each lab to manage the receipt, creation, consumption, and disposal of their inventory (defined as media, chemicals, and laboratory supplies). These labs are located strategically across the continental United States and Puerto Rico; each have FDA representation and onsite support from the application team. The material and supplier modules are foundation modules and provide support for enterprise definitions for the inventory (e.g., equipment, lab media) and organizations that source the inventory, also known as firms/ vendors. The equipment management module is a foundational module and allows the labs to manage the calibration and maintenance of the instruments used for sample testing. Finally, the labs use LIMS reports to satisfy audit requirements and support for general laboratory management.
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.	LIMS collects the following personally identifiable information (PII) from and about FDA lab personnel (FDA Employees and Direct Contractors): (a) first and last name; (b) email address and; (c) username. Email address here pertains only to FDA work email address. FDA does not share any PII in this system outside the agency. Lab personnel consist of ORA Office of Regulatory Science (ORS) Lab Analysts and Lab Supervisors. FDA does not use LIMS to collect, handle, or store PII about other external or internal individuals that are non-users. Only account holders can access the system. The PII that ORA uses in LIMS (name and email address) comes directly from the lab personnel in the form of a LIMS User Account Request Form submitted via Service Now ticket (within FDA's intranet) or an email request for a new account to an FDA Apps Desk, which also requires the completion of the form. LIMS also collects the following non-PII: (a) inventory identifier (ID), (b) date of chain of custody event, (c) Firm name and (d) Firm general contact information (i.e., general company email address, mailing address and company phone number).
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.	ORA LIMS is a Commercial Off the Shelf Laboratory Information Management System accessed by authorized lab personnel at the 13 ORA labs. The system is available on the FDA network using Single Sign On (SSO) via Smartcard Personal Identity Verification (PIV) and Active Directory (AD, a separate FDA system addressed in a separate PIA). Using LIMS, FDA codifies and automates laboratory business processes within individual ORA labs. This system supports core ORA business functions and also provides seamless and service-oriented integration with other FDA information systems within ORA. As a single integrated system, LIMS provides a unified bird's-eye view of lab activity by providing situational awareness both within individual labs and across the organization. ORA lab personnel (FDA employees and Direct Contractors) use the inventory and media foundational modules to record the receipt/creation of new inventory and other changes to the inventory/media as the inventory/media is in use in the lab. The user's name is captured and stored as part of chain of custody events. To search for inventory, the system provides a configurable query mechanism that exposes database attributes as search criteria. No PII details are configured as search criteria. Although, username is provided in the search result set. ORA lab personnel use the material and supplier modules to create audit trail records (creation, modification, username, etc.) for the firms that supply the inventory. Firm information is provided in the invoice or gathered by the ORA lab personnel from similar public sources. There is no PII related to the Firm entered in the system. The system creates an audit trail for the data entry event representing the creation of the new vendor. The name of the user who created the firm record.
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.	The purpose of the website is to access the application server. The following categories of individuals have access to the website. Only individuals who have a LIMS Account Users access the website via the intranet using SSO credentials from Active Directory.
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?	Yes
PTA - 13A:	Does the website collect PII from children under the age thirteen?	No
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?	No
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
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	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.	201 - 500

PIA - 4:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of creating user account, assigning individual as custodian for equipment maintenance and inventory monitoring. The email address is used to email the individual of equipment maintenance due, when inventory is expiring and/or when inventory needs to be ordered.
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. FDA uses the PII for testing purposes such as: testing release updates and troubleshoot issues FDA uses the PII for training purposes such as: Training is preformed when a user is new to LIMS, is granted additional role(s) after initial creating, when additional training is requested. FDA uses the PII for research purposes such as: N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The legal authorities that govern information use and disclosures specific to the system and program are: American public under the Federal Food, Drug and Cosmetic Act (21 U.S.C. 301) and the Federal Records Act (44 U.S.C. 3101) and the Public Health Service Act (42 U.S.C. 262).
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 Email Online Other
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.	Not Applicable. This does not collect information from the public that falls under the PRA definition of information collection.
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.	While submission of PII is voluntary as that term is used in the Privacy Act, there is no option to op out. The PII, including name and email address, is necessary for ORA LIMS to manage workflow and accomplish FDA mission. The user may opt out of having their email entered into the system, however, the user cannot use the system if they do not want their first and last name captured and stored.
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.	No such changes are anticipated. If FDA changes its practices with regard to the collection or handling of PII related to the LIMS system, the agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include email 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.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to resolve the situation. Employees 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). Federal, HHS and FDA policy requires all personnel to rapidly report any suspected or known compromise, exposure or other data breach involving PII.

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.	LIMS PII is provided voluntarily by the individual. The individual/supplier is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information and their PII is relevant and necessary to be granted access to the system. Integrity and availability are supported via controlled access granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Accuracy and relevance are supported through an off-boarding process in place to deactivate user accounts when users are no longer involved in LIMS or leave the agency. LIMS administrators perform annual reviews to evaluate user access. The design of form fields to collect only necessary PII further supports PII relevancy. Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authorization to operate (ATO). Controls are selected based on National Institute of Standards and Technology (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.
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 - All authorized FDA users that have LIMS Account with Material or Inventory based roles have read only access to audit trail and chain of custody. Administrators - FDA personnel and Direct Contractors supporting OIMT with the review, process and administering of the system, files and data as well as access Developers - FDA Direct Contractors support OIMT with the design, development and testing of the system. Contractors - FDA Direct Contractors support the OIMT for administration, troubleshooting and development of the system.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures in place to determine which system users may access PII are FDA users and Direct Contractors with valid network accounts who require access to LIMS must have supervisory approval by the LIMS FDA System Owner before access is granted. To get an account in LIMS, users complete an Account Request form through FDA's ServiceNow internet portal where they provide their name and email address. This information is used in setting up the account in LIMS and is used as port of the chain of custody, audit trail and email notification management.
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 following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: The LIMS FDA System Owner approves user accounts based on the information entered on the LIMS User Account Request form. The account request will be rejected if the user is requesting more access that was is necessary. The scope of access in LIMS is restricted based on role-based criteria.
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 training has been successfully completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	LIMS users are trained on the use of the system through release-specific training and ad hoc training using materials posted on the LIMS SharePoint Portal. 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).	LIMS system owners follow data retention and destruction procedures documented in the Records Management section of the LIMS Project Management Plan, NARA Citation: N1-088-05-1 The retention period will not be less than seven (7) years and FDA destroys records when no longer needed for business use, whichever is later.

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.	FDA secures PII in the system using the following administrative controls: 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. FDA secures PII in the system using the following technical controls: Technical safeguards include role-based access settings, firewalls, passwords and others. Active Directory is used for authentication. Data is encrypted in database per data center requirements. VPN is required when accessing system from remote locations. FDA secures PII in the system using the following physical controls: Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	11/27/2024
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:**	11/27/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	12/3/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/3/2024 Seems like all comments were addressed from the external review of the PIA (see Supporting Documentation). Aside from the tech issues with ATO and PTA-5A this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	6

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	There are 2 Archer issues impacting this PIA. • The Answer to PTA-5A is entered on the PTA but does not show on the PIA. • ○ PTA-5A, 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 Active Directory. You to have a LIMS account, however, to get into LIMS you need an AD account. Without an AD, you cannot get into LIMS. • This PIA is also 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 reflecting “No” as the answer when the correct answer is “Yes.” • ○ The FDA Archer Team is aware of this occurrence and is working on a solution. The FDA Archer Team is aware of this occurrence and is working on a solution.	**SAOP Review Date:**	12/4/2024
		SAOP Days Open:	1

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
11-27-2024 EMAIL_FDA PIA in Queue (OII LabOIItory Information Management System).pdf	284428	.pdf	12/2/2024 10:19 AM	0
OII LabOIItory Information Management System_SOP Approved.rtf	759365	.rtf	12/2/2024 10:19 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment

PIA - 1	BLAND, CRYSTAL	12/2/2024	There are 2 Archer issues impacting this PIA.
			• The Answer to PTA-5A is entered on the PTA but does not show on the PIA.
			•
			  ○ PTA-5A, 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 Active Directory. You to have a LIMS account, however, to get into LIMS you need an AD account. Without an AD, you cannot get into LIMS.
			• This PIA is also 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 reflecting “No” as the answer when the correct answer is “Yes.”
			  ○ The FDA Archer Team is aware of this occurrence and is working on a solution.	

			The FDA Archer Team is aware of this occurrence and is working on a solution.
PIA - 9	VILLAFUERTE, NESTOR	12/3/2024	Per PTA-5, the "Online" and "email" options should be checked. "The PII that ORA uses in LIMS (name and email address) comes directly from the lab personnel in the form of a LIMS User Account Request Form submitted via Service Now ticket (within FDA's intranet) or an email request for a new account to an FDA Apps Desk, which also requires the completion of the form. "

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:	12/4/2024 2:20 PM	**History Log:**	**View History Log**