PTA / PIA: FDA - UAC - QTR2 - 2025 - FDA4941581

Created Date: 6/18/2025 4:42 PM Last Updated: 6/25/2025 12:45 PM

General Information

PTA / PIA Name:	FDA - UAC - QTR2 - 2025 - FDA4941581	**PTA / PIA ID:**	3354128
Component Name:	FDA - CDER User Access Control Interface System	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	7
Submitter:		**Submit Date:**	6/18/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	10/21/2022
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	POC Name: Andriy Chut
PTA 01A:	POC Title and Organization	POC Title: Information Technology Specialist; Contractor POC Organization: OIMT/OTD/DAS/MPB; CDER/OTS/OCS
PTA 01B:	POC Email Address	andriy.chut@fda.hhs.gov
PTA 01C:	POC Phone Number	240-338-7846
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New

PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Food and Drug Administration (FDA) uses the Center for Drug Evaluation CDER Regulatory Tracking and Quality Management Systems for tracking, reporting, and maintaining an archival record of the drug and biological product materials submitted to the FDA for review. CDER reports to Congress on a number of issues, including performance on Prescription Drug User Fee Act (PDUFA) related goals, and CDER uses data in CDER Regulatory Tracking and Quality Management Systems for reporting purposes. This assessment addresses one component within the overall CDER Regulatory Tracking and Quality Management Systems (a collection of components addressed in multiple assessments): the CDER User Access Control (UAC) Interface System. The CDER User Access Control Interface System consists of two applications: User Access Control (UAC) and the User Access Management Automation Application (UAM). The purpose of UAC is to support the accounts management process, used to thoroughly manage system access to CDER applications. All users (administrators and application developers) are FDA Center for Drug Evaluation and Research (CDER) employees or Direct Contractors. The goal of this process is to ensure that FDA employees and Direct Contractors receive and maintain the necessary privileges in the various CDER systems, so they are able to perform their tasks efficiently. User Access Control (UAC) is the front-end application used by the CDER access team to provide access to each CDER Legacy Refresh (LX) application, Document Archiving Reporting Regulatory Tracking System (DARRTS), User Access Management Automation Application (UAM) and the UAC front end application itself. UAC provisions the level of privilege within the application. UAC is driven by a set of data tables which specify the applications in scope, the set of privileges for each application, the privileges provided to each user, and general personnel information for each user. Users: UAC users are system administrators and developers. Write access to the UAC application is strictly limited to the CDER access team. A few developers have read-only access to UAC. The User Access Management Automation Application (UAM) is an automated provisioning tool for user access. It can be considered as a modernized, phased supplement to the User Access Control (UAC) System. UAM provisions access for CDER and non-CDER employees. UAM provides a self-service web interface for CDER Designated Requestors with the appropriate authority to request user role-specific application

		access for employees within their respective office, as well as for non-CDER supervisors requesting application access for their employees. The application uses custom workflow automation to validate each request, and to provision UAC access that is “pre-approved” by the respective application owners based upon the employee role. UAM also streamlines business approval of employee access which cannot be provided by default. UAM sends the appropriate notifications to requesters, system owners, business owners, and employees. Access to UAM itself is provided through the UAC front end. UAM provides approval for following systems which are covered by separate privacy assessments: CDER Legacy Refresh (LX) Applications Document Archiving Reporting Regulatory Tracking System (DARRTS) The UAM application also facilitates approvals for access to the following non-UAC governed systems: Empirica Signal Electronic Document Room (EDR) Electronic Document Room Light System (EDRLS) CDER FDA Adverse Event Reporting System (FAERS)
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by 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 into the system are FDA Employees and Direct Contractor name, work phone number, work e-mail address, date of the request, type of employment (full-time, student intern, or direct contractor), employment start date, job title, office within the organization, FDA badge number, general area of expertise, manager's name, office director's name, and systems to which they are requesting access. This information is sent via e-mail to a UAC System Administrator who enters the information into the User Access Control System. The UAC system administrator is a member of the CDER Accounts Request team. PII collected includes name, work phone number, work e-mail address, employment status/history, and FDA badge number. Information is stored in accordance with the National Archives and Records Administration (NARA) retention schedule.
PTA 05A:	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.

PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	FDA employees and direct contractors using CDER-operated information systems use roles provisioned by UAC to receive access to information systems operated and managed within CDER. These employees complete an access which is then sent to the UAC administrators (the CDER Accounts Request Team). These UAC administrators enter the information from the access request and then use the system to create access accounts for the requesters. Requesters include new employees, transferring employees, and employees working on detail assignments. Some access requesters may not be CDER employees, but will be employed (full-time, as student interns, or as direct contractors) by other FDA Centers and offices.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://uac.fda.gov/ https://uam.fda.gov/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	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 UAC is to support the accounts management process, used to thoroughly manage system access to CDER applications. All users (administrators and application developers) are FDA Center for Drug Evaluation and Research (CDER) employees or Direct Contractors. The goal of this process is to ensure that FDA employees and Direct Contractors receive and maintain the necessary privileges in the various CDER systems, so they are able to perform their tasks efficiently. FDA Employees and Director contractors access the web site via internal FDA web portals with Single Sign-On.
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 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment		
PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name Employment Status/History Contact Information Email Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	FDA Badge Number
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	5,000 – 9,999
PIA 25:	For what primary purpose is the PII used?	PII is used to manage access to CDER applications.
PIA 26:	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 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The implementation of this system is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures of the system are required by the Federal Information Security Modernization Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	This component does not collect information using an information collection request as defined by the Paperwork Reduction Act.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Submission of PII is voluntary as that term is used by the Privacy Act. However, the submission of PII is necessary in order for users to access and use applications owned and operated by CDER. The system contains PII relevant to users' access credentials. There is no method for employees requesting application access to opt not to submit PII. Permanent employees, direct contract employees, fellows and other personnel must provide their PII in order for the Agency to process administrative materials and securely administer access to Agency information.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the web site, or e-mail notice to the individuals.
PIA 36:	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.	Users who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to raise their concerns. They can work with their supervisor(s), a 24-hour FDA technical assistance line, FDA's Cybersecurity Infrastructure Operations Coordination Center (CIOCC), the FDA Privacy Office and other offices.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	All FDA personnel, including users of this application, are responsible for providing accurate information and may independently update and correct their information at any time. All information is relevant to the authentication and authorization process. Integrity and availability are protected by security safeguards selected based on guidance from the National Institute of Standards and Technology (NIST) appropriate to the level of risk associated with the application.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	UAC users are system administrators and developers. Write access to the UAC application is strictly limited to the CDER access team. A few developers have read-only access to UAC. Contractors: Some HHS Direct Contractors are system administrators or developers.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Management (the system owner and administrators) establishes roles for individual personnel for each CDER application, with technically and administratively enforced role-based restrictions permitting access only to information that is required for each individual to perform his/her job.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Access to Personally Identifiable Information (PII) is governed by the principle of least privilege. When a user account is created, the user's supervisor specifies the minimum level of system access required for the individual to perform their job duties. This ensures that users are only granted access to the specific data necessary for their roles. Access permissions are regularly reviewed to maintain compliance with this principle. During these reviews, accounts that are no longer required are removed from the system.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All personnel must complete FDA's mandatory Computer Security Awareness Training at a minimum of every twelve months. This course includes privacy awareness training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users, however, additional on-the-job or informal training may be received and privacy guidance is available on the FDA intranet and from Privacy staff.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Records are managed in accordance with National Archives and Records Administration (NARA) general records schedule (GRS) 3.2, Item 030-System Access Records. Disposition: TEMPORARY. Destroy when business use ceases.
PIA 45:	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; Single Signon (SSO) protocols; 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 and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/18/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/18/2025
SOP Review 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.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/25/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/25/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	7

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/25/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/25/2025 8:08 AM	BLAND, CRYSTAL	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	6/23/2025	6/23/2025 Per FDA's email: The PIA is experiencing an Archer error with question General 03: "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 *10/21/2022*. • At this time, we are unable to update Archer to reflect the correct answer "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution.	CDER User Access Control Interface System PIA_SOP Approved.pdf 6-18-2025 EMAIL_PIA In Queue (CDER User Access Control Interface System).pdf