PTA / PIA: FDA - OCSC - QTR3 - 2025 - FDA4949866

Created Date: 8/4/2025 12:42 PM Last Updated: 8/5/2025 12:43 PM

General Information

PTA / PIA Name:	FDA - OCSC - QTR3 - 2025 - FDA4949866	**PTA / PIA ID:**	3599270
Component Name:	FDA - CDER OCS Connect Service Desk	**ATO Boundary Name:**	CDER Study Data Review Tools
Overall Status:	Complete	**# of Days - Open:**	1
Submitter:		**Submit Date:**	8/4/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	FDA
Security Categorization:	Low		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
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.	12/31/2025
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	Setondji Dega
PTA 01A:	POC Title and Organization	Project manager, CDER/OCS/DRRR
PTA 01B:	POC Email Address	Setondji.Dega@fda.hhs.gov
PTA 01C:	POC Phone Number	(240) 838 2014
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's (FDA) Center for Drug Evaluation and Research (CDER) Office of Computational Science (OCS) Connect is a component of the CDER Study Data Review Tools (SDRT) system. The SDRT system is comprised of several individual applications and components that are each addressed in their own respective Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA)'s. CDER OCS Connect provides a centralized hub of information, resources, training, and analytical support to CDER reviewers and the Scientific Computing community to efficiently and effectively utilize OCS tools and services.
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.	CDER OCSD collects the following Personally Identifiable Information (PII): First and last names, and work email addresses for FDA employees and Direct Contractors. The PII in these systems is not shared with any other system or organization. Users access this system via an FDA-only internal web pages. This system grants users access using the Single Sign-On (SSO) process via FDA's Active Directory (the subject of a separate PIA). Users of SDRT (FDA employees and Direct Contractors) do not use any personal identifiers to retrieve records held in the system. PII is stored in the system in accordance with the National Archives and Records Administration (NARA) records retentions standards.
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.	The information about users' name, email, and department is collected and/or maintained in order to generate system performance and understand the traffic generated. PII from the CDER OCS Connect users is shared with leadership for communication purposes.
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://ocsconnect.fda.gov/#/home
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 OCS Connect Portal is an enterprise system designed to connect CDER review communities with the services, tools, training, and innovative solutions essential for facilitating regulatory review activities. The OCS Connect@Nexus central platform automates and streamlines access to resources through intelligent Appian workflows, enhancing interactions between reviewers and solution providers. Users can access via internal website log in with Single Sign-On (SSO).
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 Contact Information Email Address (Business)
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.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose of the PII used in the CDER OCSD system is to identify points of contact consisting of FDA employees and Direct Contractors for account management and to communicate operational information.
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.	Food Drug, and Cosmetic Act, 21 U.S.C. 301; 45 CFR Part 46 Subpart A.
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 Hard Copy Mail/Fax Email Online

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?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	The PII is shared and disclosed with leadership for communication purposes and to track system performance.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Not applicable (N/A)
PIA 32D:	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.	The SDRT tools use individual role-based accounts to ensure minimum necessary access. Each tool maintains an access control procedure which outlines the steps to request role-based access. The roles include, at a minimum, "administrator" and "user." Other roles include variations of the user role. The system, business, and/or data owner will authorize access to the system with supervisory approval. The administrator of the system will set the appropriate degree of access. All users are authenticated by FDA enterprise-wide SSO, Active Directory, or username/password combination. Once a user is authenticated by FDA, credentials are passed to the tool, and the tool will provide access based on the role.
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.	There is a warning that gives users option to accept or reject the fact that any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose. There are no opt-out procedures specific to OCS Connect. If users elect not to provide this information, it may impact the FDA related work they are required to do per their duties.
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.	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 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). Employees may also report suspected data breaches and obtain assistance through ERIC, FDA's CIOCC, and FDA's Privacy Office. U.S. Department of Health and Human Services (HHS) and FDA policy obligates all permanent and Direct Contractor personnel to rapidly report suspected breaches. Within FDA, all reports of suspected breaches must be reported to the CIOCC.
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.	Individuals voluntarily provide their PII. Since this is done on the backend by using automatic process to capture user information, it is not error prone. PII relevancy is supported through the design of the system to require and collect only the PII elements necessary to administer the system and enable its intended use. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by privacy and 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.
PIA 38:	Identify who will have access to the PII in the system.	Users 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.	Users-service providers need access to the system to improve their services based on user behavior and activities. Developers-Developing the system to improve the platform. Contractors: Some HHS Direct Contractors are users and developers.

PIA 40:	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 submit a request with valid justification 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 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.	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. Technical controls and settings are applied to enforce role-based access limits.
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 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 43:	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 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).	PII in the OCS Connect System covered under General Records Schedule 3.2 “Information Security Systems Records”, Item 31 “systems requiring special accountability for access.” The disposition instruction is to destroy 6 years after password is altered, or user account terminated but longer retention is authorized if required for business needs.” Disposition: Temporary under DAA-GRS-2013-0006-0004.
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 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 and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	8/4/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/4/2025
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:**	8/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/5/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/5/2025
SAOP Review Comments:	Approved on behalf of the SAOP	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/5/2025 10:03 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	8/4/2025	8/4/2025 PER FDA's Email, The planned ATO date is 12/31/2025.	8-4-2025 EMAIL_PIA in Queue (CDER OCS Connect Service Desk).pdf CDER OCS Connect Service Desk PIA_SOP Approved.pdf