Privacy Impact Assessment (PIA): FDA - CDER DC - QTR4 - 2024 - FDA4089322

Created Date: 10/1/2024 4:22 PM Last Updated: 10/23/2024 1:45 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 - CDER DC - QTR4 - 2024 - FDA4089322	**PIA ID:**	2278716
Name of Component:	FDA - CDER Data Central	**Name of ATO Boundary:**	CDRH Scientific and Research General Support Systems
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	22
Submission Status:	Submitted	**Submit Date:**	10/1/2024
Next Assessment Date:	10/23/2027	**Expiration Date:**	10/23/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4089322
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.	1/10/2023
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.	Since this Privacy Threshold Analysis/Privacy Impact Assessment was last approved, the Food and Drug Administration (FDA) made the following changes to the system: Migrated from the previous identity authentication process where access to the system was provided via login by email address (username) and a self-created password. These credentials were PII and stored in the system in an encrypted format. Implemented a new, network-level, multi-factor, single sign-on (SSO) process for controlled user authentication and access. The system no longer uses or stores system-specific user credentials (email address and password). Once a user is successfully authenticated by FDA SSO, Office of Computational Science (OCS) Data Central System provides access based on user role, controlling access to data and system functionalities.
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 purpose of the Center for Drug Evaluation and Research (CDER) Office of Computational Science (OCS) Data Central system is to display, migrate, watch, and identify drug and biologic applications from Electronic Data Room (EDR) each day into a centralized repository in support of the FDA Drug Review Process. OCS Data Central also collects and displays metadata about these drug and biologic applications. This system receives data from other internal FDA systems: EDR, Document Archiving, Reporting and Regulatory Tracking System (DARRTS), and Office of Business Informatics (OBI) Metadata Database (also known as Integrity). The system also exchanges data with other internal systems consisting of CDER Nexus and CDER's Appian workflow system. The system also shares data with other FDA systems and tools including Line Listing Tool, MedDRA Adverse Event Diagnosis (MAED), Analysis Studio, Janus, SAS Analytics Remote Grid Environment (SARGE), and DataFit. FDA assesses all of these other systems in separate privacy impact assessments (PIAs). This system enables access to study data by FDA CDER users, namely Reviewers (of regulated drug product submissions), statisticians, analysts, and data managers, by connecting to OCS Tools and Services and providing access to usable data. The initial set of primary users are the OCS Data Management team and the OCS Tools and Services teams. This system is hosted in the FDA Data Center in Ashburn, VA.

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.	OCS Data Central stores and shares both personally identifiable information (PII) and non-PII data. OCS Data Central stores the following PII about Clinical Investigators (primarily business, not personal, in nature): (a) name, (b) e-mail address, (c) phone number, (d) fax number, and (e) mailing address. Clinical Investigators perform drug and biologic clinical trials in support of new drug and biological license applications. Apart from the OCS Data Central data management team, this PII is shared with the OCS Clinical Services (a service offered by the CDER/OCS organization) and FDA's Site Selection Tool teams and their constituents, Reviewers, and statisticians within FDA CDER. OCS Data Central also stores the following PII (business, not personal, in nature) about product/trial Sponsors: (a) name, (b) e-mail address, (c) phone number, and (d) mailing address. Other than the OCS Data Central data management team, this PII is shared with the OCS Tools and Services teams and their constituents, Reviewers, and statisticians within FDA CDER. OCS Data Central also stores the following categories of non-PII data: (a) drug data (drug identifier information), (b) file names within submissions, and (c) Application Reports (e.g., drug labeling data), and (d) Study Data Reports. This non-PII is shared with the OCS Tools and Services teams, including OCS Clinical Services, Site Selection Tool, Line Listing Tool, MAED, Analysis Studio, Study Data Platform, SARGE, CoreDF, and FLARe. In addition to OCS Tools and Services teams, the user community includes their constituents, namely Reviewers and statisticians within FDA CDER. The OCS Data Central system support team consists of data managers, developers, and system administrators who are FDA CDER/OCS Direct Contractors. OCS Data Central has a network-level, multi-factor, single sign-on (SSO) process for controlled user authentication and access. Once a user is successfully authenticated by FDA SSO, OCS Data Central System provides access based on user role, controlling access to data and system functionalities.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card

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.	OCS Data Central displays new drug and biological license application information to users, migrates that data to and from other internal-facing agency systems and tools, watches for incoming submissions and sends alerts to users when there is a new submission and identifies applications stored in CDER's Electronic Data Room (EDR). It thereby serves as a centralized repository of new drug and biological license application data. The PII in the system consists of contact information about Clinical Investigators and Drug Sponsors. The primary purpose of the Clinical Investigator PII in the OCS Data Central System is to identify the Clinical Investigators at the sites for use in potential site selection and inspection processes. The primary purpose of the Sponsor PII in the OCS Data Central system is to identify the point of contact at a drug company and enable any required follow up regarding its drug application. CDER OCS personnel who directly access and use the OCS Data Central system do not use any personal identifiers to retrieve records held in the system. OCS Data Central System uses role-based security, determined by the business needs of the user, to ensure minimum necessary access. The system has three user roles, which cannot be combined. End-User/Reviewers have access to system data associated with their respective FDA Center. Super-Users have view access to all system data regardless of FDA Center. Administrators have view access to all system data regardless of FDA Center, to update registry data, manage system accounts, and review access logs. OCS Data Central has a network-level, multi-factor, single sign-on (SSO) process for controlled user authentication and access. Once a user is successfully authenticated by FDA SSO, OCS Data Central System provides access based on user role, controlling access to data and system functionalities. There is no use of a mobile application associated with the system at this time.
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 enable access to study data by FDA CDER users, namely reviewers (of regulated drug product submissions), statisticians, analysts, and data managers, by connecting to OCS Tools and Services and providing access to usable data. The following categories of individuals have access to the website: OCS Data Management team, OCS Tools and Services teams, and approved FDA reviewers, statisticians, analysts, and data managers. Users access the website via a network-level, multi-factor, single sign-on (SSO) process for controlled user authentication and access. Once a user is successfully authenticated by FDA SSO, OCS Data Central System provides access based on user role, controlling access to data and system functionalities.
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 Email Address Phone numbers Mailing Address User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	The primary purpose of the Clinical Investigator PII in the OCS Data Central System is to identify the Clinical Investigators at the sites for use in potential site selection and inspection processes. The primary purpose of the Sponsor PII in the OCS Data Central system is to identify the point of contact at a drug company and enable any required follow up regarding its drug application.
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.	Food Drug, and Cosmetic Act, 21 U.S.C. 301; 45 CFR Part 46 Subpart A.
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.	Government Sources Within the OPDIV Other HHS OPDIV Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes

PIA - 10A:	Provide the information collection approval number.	The OMB information collection approval number is OMB Control No: 0910-0130, expiration 12/31/2026.
PIA - 10B:	Identify the OMB information collection approval number expiration date.	12/31/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
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.	Submitters provide their contact information as a practical requirement in order to communicate with FDA and to gain access to the system. There are no opt-out procedures specific to OCS Data Central. While FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity. Furthermore, the OCS Data Central system is not the system that serves as the original point of collection.
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 changes its practices with regard to the collection or handling of PII related to the website, 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 e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.

PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	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). Employees may also report suspected data breaches and obtain assistance through ERIC, FDA's CIOCC, and FDA's Privacy Office. 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 - 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.	Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. 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. CDER/OCS performs annual reviews to evaluate user access.
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-Developing the system to improve the drug approval process. Administrators-Developing the system to improve the drug approval process. Developers-Developing the system to improve the drug approval process. Contractors-Direct Contractors require access when developing the system to improve the drug approval process.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	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 - 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).	Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's Privacy Office.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	PII in the OCS Data Central 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.” The disposition authority is under DAA-GRS-2013-0006-0004.

PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	10/1/2024
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:**	10/1/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/3/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 10/3/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	PIA is currently 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."	**SAOP Review Date:**	10/23/2024
		SAOP Days Open:	20

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(10-1-2024) EMAIL_PIA in Queue (CDER Data Central).pdf	360013	.pdf	10/2/2024 8:48 AM	0
CDER Data Central_SOP Approved.pdf	174766	.pdf	10/2/2024 8:50 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	10/3/2024	Per FDA's Email (see Supporting Documentation) This PIA is currently 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.”	

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:	10/23/2024 1:45 PM	**History Log:**	View History Log