Privacy Impact Assessment (PIA): FDA - CDER NEXUS PTS - QTR3 - 2024 - FDA3562142

Created Date: 8/16/2024 8:03 AM Last Updated: 8/22/2024 3:11 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 NEXUS PTS - QTR3 - 2024 - FDA3562142	**PIA ID:**	2123701
Name of Component:	FDA - CDER Nexus	**Name of ATO Boundary:**	CDRH Scientific and Research General Support Systems
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	8
Submission Status:	Submitted	**Submit Date:**	8/15/2024
Next Assessment Date:	N/A	**Expiration Date:**	8/22/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA3562142
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	5/26/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

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.	FDA has made no changes to this component since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
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 Center for Drug Evaluation and Research (CDER) Nexus system is a component of the larger CDER Regulatory Review (CDER RR) system. Food and Drug Administration (FDA) has addressed CDER RR in multiple Privacy Impact Assessments (PIAs); this is one such PIA. The system is a platform designed to enable implementation and modernization work. The CDER Nexus platform modernizes the human drug review workflow by improving throughput, transparency, and enabling knowledge management within FDA and CDER. CDER Nexus is an instance of Appian, which is a vendor managed cloud solution called a Platform-as-a-Service (PaaS), hybrid cloud application. Appian is the business process management (BPM) tool of choice to help aide with modernization efforts at CDER. CDER uses the system to address the business needs of CDER's core sets of work processes supporting pharmaceutical quality, drug safety, regulatory review, and business 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.	The CDER Nexus system collects the following personally identifiable information (PII) about FDA employees, Direct Contractors and employees at pharmaceutical companies (members of the public): Employee name, office/work email address, office/work phone number, office/work mailing address. For external individuals, the system collects the same contact information PII plus access credentials (system-specific username and password). The collected PII is not shared with any other system or organization and is maintained internally within FDA. The system also collects the following non-PII elements: Internal safety meeting date and time, whether a submission has a waiver, application type and number, and submission type and 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.	CDER Nexus employs the Appian PaaS, a hybrid cloud application providing business process management (BPM) capabilities that assist FDA in achieving requirements of the CDER Business Modernization efforts. CDER Nexus is a platform designed to enable implementation work. The CDER Nexus platform has modernized the human drug review workflow by improving throughput, transparency, and enabling knowledge management. The PII collected in CDER Nexus is limited to that which is necessary and used to administer and control system access and use. Internal users of the CDER Nexus System consist of authorized FDA employees and Direct Contractors. External users consist of personnel employed by FDA-regulated external entities (e.g., drug manufacturers) who submit information to CDER on behalf of their employers. PII collected about FDA personnel and Direct Contractors is obtained from FDA's Active Directory system, the subject of a separate PIA. PII pertaining to external individuals comes through the CDER NextGen portal application that is addressed in a different PIA. External users do not have access to any information other than that which they submit. There are two account types that are for the internal users of the system: Application/submission and safety tracking. The application/submission account type is used for FDA employees, Direct Contractors, chief project management staff, regulatory project manager, discipline team lead and reviewers. The safety tracking account is used for FDA employees, Direct Contractors, signal identifier, safety lead, signatory authority, project manager, and review team member. Only work context PII is collected, and is limited to the names, access credentials (username and password for external individuals only), email address, phone number, and mailing address. CDER personnel who access or use the system must do so using multi-factor authentication through a network level, single sign-on (SSO) process. CDER personnel who access or use the system do not use personal identifiers to retrieve records held in the system.
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?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	

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.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
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?	
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?	
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.	Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	The PII collected and/or handled in CDER Nexus is used to manage implementation work for modernization actions and to control access to the system. Names, email address, phone number, and mailing addresses are collected to enable CDER Nexus to contact an individual regarding a submission made for a new drug application or to contact an individual at a facility used to manufacture the drug.
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.	The legal authorities that govern information use and disclosures specific to the system and program are: Provisions of the Federal Food, Drug & Cosmetic Act at 21 U.S.C. 301 including sections 353, 355, 356b, 360.
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 Online Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Not Applicable (N/A)-Not subject to PRA
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.	Although submission of PII is "voluntary," individuals are not provided a specific opt-out method. PII is necessary for employment and performance of duties involving Nexus use, and, for submission of materials and related communications, and for log on and controlled access the system.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	No such changes are anticipated. If the FDA or CDER changes its practices regarding the collection or handling of PII related to the CDER Nexus 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 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.	There is no process in place specific to CDER Nexus. Individuals may contact the FDA CDER Office of Business Informatics (OBI) or management, the FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), and/or the FDA Privacy Office. Privacy Office contact information is available on FDA's internet and intranet.

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.	To ensure accuracy and relevancy of their PII, CDER Nexus users may correct/update their information themselves. Their PII is relevant as necessary to be authenticated and granted access to the system. Relevancy is further ensured through the design of the system to gather only the necessary PII. This assessment also enforces collection of only the PII that is essential. Integrity and availability are protected by privacy and security controls selected and implemented during providing the system with an authority 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. CDER performs annual reviews to evaluate user access. Data integrity and availability are also supported by information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered.
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: Will have access to their own PII in the system and can edit it for changes. Administrators: Will have access to user PII when needed for account management purposes. Developers: Will have access to user PII for system development, implementation, and operations and maintenance tasks. Contractors: Some of the Developers are Direct Contractors

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	A systems administrator is the only individual who can grant access to a system, and there must be a valid reason for having access to the system (only individuals who will be reviewing submission need access) to a system. Accounts are set up using an internal approval process. The internal approval process requires that each employee's supervisor provide written justification to CDER Nexus administrators substantiating the user's need to have access. External users do not have access to PII other than their own.
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.	User-level authorization and authentication systems are in place regarding internal users. Internal users may request access to PII in the system to perform their official duties and must obtain supervisor approval. Via technical role-based account settings, external users may only access their own PII that they submit when accessing the CDER Nexus system.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	FDA personnel including Direct Contractors are required to complete FDA's mandatory security and privacy awareness training annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	A training session, as well as user guides showing how to use CDER Nexus (CDER Nexus) system are provided to all users of the system. There is also a user guide/video that provides step-by-step instructions for the use of the CDER Nexus application.
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).	FDA maintains records in accordance with the following Nation Archives and Records Administration (NARA) General Records Schedules (GRS): GRS 3.2: Information System Security Records Item 30: System Access Records – systems not requiring special accountability for access The GRS disposition authority is DAA-GRS¬2013-0006¬0003 with the records being destroyed when business use ceases. Item 40: System backups and tape library records – incremental backup files The GRS disposition authority is DAA-GRS¬2013-0006¬0005 with the records being destroyed when superseded by a full backup, or when no longer needed for system restoration, 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.	The administrative safeguards applied include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Applied technical safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include maintenance of data servers 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:**	8/15/2024
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:**	8/16/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/19/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte The comments have been addressed. This PIA is read for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	3

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	8/22/2024
		SAOP Days Open:	3

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	8/19/2024	Reviewer notes that it is stated that the system does not have an ATO, however, there is a date provided with the planned ATO date which has already passed. Please verify the ATO status. PIA-1 - Please add "Name" as one of the PII elements collected per PTA-5.	
PIA - 1	BLAND, CRYSTAL	8/19/2024	Per PTA-5, please add "Phone numbers" as one of the PII elements collected.	

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:	8/22/2024 3:11 PM	**History Log:**	View History Log