Privacy Impact Assessment (PIA): FDA - NGP - QTR1 - 2025 - FDA4915287

Created Date: 3/20/2025 4:26 PM Last Updated: 3/25/2025 1:54 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 - NGP - QTR1 - 2025 - FDA4915287	**PIA ID:**	2892740
Name of Component:	FDA - CDER NextGen Portal	**Name of ATO Boundary:**	CDER Regulatory Review
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	5
Submission Status:	Submitted	**Submit Date:**	3/20/2025
Next Assessment Date:	N/A	**Expiration Date:**	3/24/2028
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4915287
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)?	Yes
4:	ATO Date or Planned ATO Date.	5/26/2022
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 Food and Drug Administration (FDA) has made no changes to this system/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) NextGen Portal (NGP) system is a strategic initiative of the Food and Drug Administration (FDA). It enables the creation of a Government-to-Business (G2B) web application portal (https://cdernextgenportal.fda.gov/) that allows pharmaceutical industry users to submit Drug Shortages, Pre-Abbreviated New Drug Application (ANDA) meeting requests, Control Correspondence, Company Affiliation Program Fee, Pre-Assignment, Drug Development Tools (DDTs), and other information for the FDA to evaluate. In some circumstances, FDA users are also allowed to enter this type of data on behalf of industry users. The CDER NGP project has put in place a portal to capture and submit various types of data from industry, government, and other sources. NGP receives a daily data feed from CDER Integrity (a CDER system assessed in a separate PIA) which is used by CDER to determine pharmaceutical companies' compliance with FDA regulations for reporting shortages of drugs and requesting pre-ANDA meetings. Users of the NGP system consist of FDA employees and Direct Contractors (internal users), and employees or representative of pharmaceutical industry/organizations (external users). Okta is an external enterprise-grade, identity management service, built for the cloud, but compatible with many on-premises applications. The Okta solution provides a multi-factor authentication (MFA) capability that increases the strength of user passwords while providing Single Sign-On (SSO) capability for the NGP applications/modules. FDA personnel use Okta to manage access to applications and devices. Okta is also employed with Oracle Internet Directory (OID) as a directory service based on the Lightweight Directory Access Protocol (LDAP) used for on premises user authentication. Okta is a FedRAMP and FDA approved third-party identity management tool. It employs an external LDAP structure that sits outside of the NGP system and handles user information (email, phone number, first name, last name, middle name, and unique person ID) as necessary for authentication and identity management functions.
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.	Information collected by NGP is stored using Oracle database technology in the Amazon Web Services (AWS) GovCloud environment. Below is the information collected for each of the different use cases: Meeting request data handling includes non-PII information related to listed drugs and business justifications for the meeting request. The PII collected includes requester information which typically consists of pharmaceutical company employee name, office email, office phone number, and office mailing address.

Drug shortages data collection includes PII consisting of the facility point of contact's first and last name, office email address, office phone number, and office mailing address. The non-PII collected includes facility name and business justification for the facility regarding an inability to manufacture drug products.

Controlled Correspondence use collects non-PII which includes facility information consisting of facility name, address and DUNS number. Other forms of non-PII collected include product information, inactive ingredients and business justification for the controlled correspondence. Controlled Correspondence use also collects the following PII in order to contact individuals for correspondence in reference to drug information: first and last name, office mailing address, office phone number and office email address.

Company Affiliation Program Fee use does not involve PII collection. It includes collection of non-PII consisting of company name, address and Data Universal Numbering System (DUNS) number. Other forms of non-PII collected include ANDA products and application holder information (new drug application as requested by a facility only), and associated ANDAs to determine program fee categorization.

Pre-Assignment Number use of NGP collects non-PII consisting of business name, business address, DUNS number, product information, and business justification for retrieving a pre-assignment number. This use of NGP does not entail handling PII.

NGP use for Drug Development Tools (DDTs) collects non-PII data consisting of business name, address, DUNS number and business justification for submitting a DDT. PII about points of contact and partners is collected and includes first and last name, company name, office mailing address, office phone number and office email address.

The PII collected about all users (both internal and external) of the system consists of first name, last name, office phone number, office mailing address, and a valid office email address. As part of authentication, additional PII is collected and consists of access credentials (username/password), work/office email address (often the username), security image (user selected image for authentication purposes), and a security question and answer (for password resets). Internal users, FDA employees and Direct Contractors, will select FDA as the company while external users will select (or manually enter) their organization's details including organization name, firm address and DUNS number (if applicable).

Okta/Oracle Internet Directory (OID), as part of the Identity Management capability, receives PII about users directly from FDA's NGP (valid email address,

		work phone, first name, last name, middle name, unique-person-ID) as stored in NGP. NGP will transmit all the above-mentioned fields to Okta. Once an account is created/activated in Okta, Okta will also store user password, security image, and security question chosen by the user (the user must select a security question from a drop-down menu while activating the account). For system login, users provide their office email address, password, and 6-digit multi-factor authentication (MFA) code received via e-mail. All traffic between NGP and Okta is encrypted using FIPS 140-2 encryption.
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 Email Address Non-HHS User Credentials Password
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.	NGP is a Government to Business (G2B) web application portal (https://cdernextgenportal.fda.gov/), designed to collect information from pharmaceutical companies for the following events: Drug Shortages, Pre-ANDA meeting request, Control Correspondence, Company Affiliation Program Fee, Pre-Assignment, Drug Development Tools (DDTs). Using a web portal, pharmaceutical industry users can submit pre- ANDA meeting requests, drug shortages, Control Correspondence, Program Fee, Pre-Assignment, and DDT information for FDA evaluation. There are some instances which provide the capability for internal FDA NGP users to enter this type of data on behalf of industry users. CDER utilizes NGP to determine pharmaceutical companies' compliance with FDA regulations for reporting data for the events. The PII collected for all users (internal and external) of the system includes: First Name, Middle Name, Last Name, Phone Number, a valid Email Address, user-password, security image, 6-digit multi-factor authentication code (provided via e-mail during the login process), and a security question and answer (for password resets). Internal users, FDA employees, and Direct Contractors will select FDA as the company while external users will select (or manually enter) their organization's details including Organization Name, Address and DUNS number (if applicable). Username, password, 6-digit multi-factor authentication code (provided via e-mail during the login process) are collected from the users when authenticating into the NGP application. Records in NGP are not retrieved by name or other personal identifiers.

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)?	Yes
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 website (https://cdernextgenportal.fda.gov/) allows pharmaceutical industry users to submit Drug Shortages, Pre-ANDA meeting request, Control Correspondence, Company Affiliation Program Fee, Pre-Assignment, and Drug Development Tools (DDTs) information for the FDA to evaluate. In some circumstances, FDA users are also allowed to enter this type of data on behalf of industry users. Users of the NGP system consist of FDA employees and Direct Contractors (internal users) and employees or representatives of pharmaceutical industry/organizations (external users). FDA employees/Direct Contractors access the system using Single Sign-On (SSO) with their HHS/FDA PIV cards. The external users access the system via URL and enter a non-HHS username and password. The PII collected about all users (both internal and external) of the system mainly consists of business contact information. Only the minimum necessary FDA employees and Direct Contractors have access to this PII.
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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - 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 Photographic Identifiers 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.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The PII collected and/or handled in NGP is used to manage pharmaceutical entity compliance submissions and to control access to the system. The PII is mainly used for business contact purposes.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Not applicable. There are no secondary uses for 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.	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 Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
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.	CDER NextGen Portal does not need OMB approval because this is not an information collection request as defined by the Paperwork Reduction Act.
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.	PII is necessary to establish an NGP login for users to access the system and to enable communications, and there is no option to opt-out. If a user does not provide their PII, they will be unable to use the NGP.
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 NGP 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.	If an NGP user believes that their PII is inaccurate, they can update the information themselves in the NGP. They may also contact the CDER NGP point of contact to receive technical assistance to update their information in the system. If an NGP user believes that their PII has been inappropriately obtained, used, or disclosed, they can report any known or suspected breaches to the FDA Privacy Office as well as the FDA's Cybersecurity and Infrastructure Operations Coordination Center (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.	To ensure accuracy and relevancy of their PII, CDER NGP 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 this assessment that enforces collection of only the PII that is essential. Integrity and availability are protected by 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 and adjust 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.	Administrators 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.	PII access is required by contractors and administrators to assist with troubleshooting efforts and provide technical support.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). External industry users submit access requests through the Government-to-Business (G2B) web application portal (https://cdernextgenportal.fda.gov/). Upon receiving a request for the creation of an external industry user account, FDA administrators contact the company to verify the requesting user's company of employment and whether the user is authorized to submit data to the FDA on behalf of the company. FDA administrators are responsible for managing end user accounts for external industry users. All other internal FDA user accounts (administrators, developers, or Direct Contractors) are set up using an internal approval process. The internal approval process requires that each employee's supervisor provide written justification to NGP administrators substantiating the user's need to have access.
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 for external and 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 NGP 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 annual Computer Security Awareness Training (CSAT).
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	A user guide/video provides step-by-step instructions for the use of the NGP application and is available on the NGP portal (https://cdernextgenportal.fda.gov/).

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 NGP 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. Item 41: System backups and tape library records – fully backup files The GRS disposition authority is DAA-GRS2013-0006¬0006 with the records being destroyed when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later. Item 51: Backup of master files and databases – temporary records The GRS disposition authority is DAA-GRS¬2013-0006¬0008 with the records being destroyed immediately after the identical records have been deleted or replaced by a subsequent backup file, but longer retention is authorized if required for business use. GRS 5.2 Intermediary Records with the disposition authority of DAA-GRS-2017-0003-0002. In addition, CDER NGP uses the following CDER file codes: 5120 which cover database records, 2310 which deletes or destroys records 30 years after cutoff or when no longer needed for reference or research, whichever is later, and 2330 which destroys the records 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.

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 employed include a user guide, system documentation that advises on proper use, and implementation of Need to Know and Minimum Access Necessary principles when awarding access. Technical Safeguards include identity badges, multi-factor authentication, usernames and passwords, and role-based access permissions. Physical controls include that all system servers are located at FDA-governed 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:**	3/20/2025
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:**	3/20/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/24/2025
Agency Privacy Analyst Review Comments:		**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	3/25/2025
		SAOP Days Open:	1

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	3/21/2025	Reviewer noted that PTA-12A states that Session Cookies collect PII.	

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:	3/25/2025 1:54 PM	**History Log:**	View History Log