PTA / PIA: FDA - Direct - QTR2 - 2026 - FDA5271033

Created Date: 6/3/2026 6:00 PM Last Updated: 6/8/2026 6:00 PM

General Information

PTA / PIA Name:	FDA - Direct - QTR2 - 2026 - FDA5271033	**PTA / PIA ID:**	4543120
Component Name:	FDA - CDER Direct	**ATO Boundary Name:**	CDER Direct
Overall Status:	Complete	**# of Days - Open:**	5
Submitter:		**Submit Date:**	6/3/2026
Next Assessment Date:	06/07/2029	**Expiration Date:**	6/7/2029
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
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.	11/18/2025
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	Hanming Tu
PTA 01A:	POC Title and Organization	Title: Advisor / Business Informatics Specialist Organization: FDA/OO/OBI
PTA 01B:	POC Email Address	hanming.tu@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-3881
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	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 component since the last Privacy Threshold Analysis (PTA) /Privacy Impact Assessment (PIA) was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Food and Drug Administration (FDA) Center for Drug Evaluation and Research (CDER) Direct system is a web-based submissions portal designed to help the pharmaceutical industry seamlessly create, submit, and manage their Health Level 7 (HL7) Structured Product Labeling (SPL) submissions. In support of the Department of Health and Human Services (HHS) mission, CDER Direct enables regulated industry entities to fulfill their legal obligations related to drug establishment registration and drug product listing, thereby supporting FDA's broader mandate to protect and promote public health through the regulation of pharmaceutical products. The system carries out its functions through three core components. First, it provides a web-based portal to support HL7 SPL and Self-Identification (Self-ID) submissions. Second, it operates a backend system to store and archive Extensible Markup Language (XML) and relational data. Third, it includes an integration bridge that communicates with the Electronic Listings (eList) system for HL7 SPL submission validation and acceptance. When a user submits data, the system generates SPL in the background and creates the submission on the file system. A MOVEit server then picks up the submission and forwards it to the eList system for validation. If the submission passes validation, it is sent to the Drug Quality and Compliance Program (DQCP) system for processing, and the submission status is updated to "Submission Accepted." If errors are found, the submission status is changed to "Validation Failed," and the user is notified so that corrections can be made and the submission resubmitted. The users of CDER Direct are largely external, consisting primarily of members of the pharmaceutical industry who submit SPL documentation to the FDA. External users register through the CDER Direct public-facing portal at https://direct.fda.gov using their organization's Data Universal Numbering System (DUNS) number. Upon submitting a registration request, the system sends a confirmation email to the user, who then sets their username and security answers and is assigned all administrator roles for their organization. These users can create, update, modify, activate, and deactivate access to forms for sub-accounts within their organization, though they are restricted to viewing only their own organization's submissions. Internal FDA users, such as site administrators, access the system through a separate administrative application located on the FDA

		intranet at https://dqcp.fda.gov, using Single Sign-On (SSO) with Multi-Factor Authentication (MFA). Internal administrators are approved by the Business Owner and have a limited set of privileged functions, including resetting user passwords, activating or inactivating user accounts, creating administrator accounts when necessary, and viewing access logs and system parameters. The system is currently in the Operations and Maintenance phase of its System Development Life Cycle (SDLC) and is classified as a Major Application with a Moderate security categorization.

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The system contains Drug Establishment Registration data as required by the Food, Drug and Cosmetic Act (FD&C Act), 21 U.S.C. §360(b)-(d). This data includes Personally Identifiable Information (PII) in the form of the first and last name, work phone number, and work email address of points of contact for organizations in the pharmaceutical industry. Additionally, for account creation purposes, industry submitters are required to enter their work mailing address, work email address, work contact number, and job title, all of which are considered PII when combined with name or other unique identifiers. Usernames and self-created passwords for industry submitters are also housed within the system and are considered PII. Notably, CDER Direct contains no PII about FDA employees or Direct Contractors, as FDA employees access the system through Active Directory using the SSO process and no system-specific authentication credentials are stored in CDER Direct for them. The system also maintains non-PII data, including the name and mailing address of the submitting organization, as well as the organization's DUNS number (in this instance it is not being used to identify individual proprietors). Furthermore, the system maintains Drug Label and Drug Listing Data for each drug required to be reported under 21 U.S.C. §360(j) of the FD&C Act. This includes each drug's name, National Drug Code (NDC) Directory number, ingredients, and other similar characterizing information, all of which is considered non-PII. Industry submissions are archived in the system following an FDA General Retention Schedule (GRS). Records are retained under the schedule tracked by the National Archives and Records Administration (NARA) Approved Citation N1-88-07-2, under FDA File Codes 7220/7222 (Compliance (Agency-Wide); Registration and Listing Systems; Database Records). Records are maintained until a "cutoff date," which occurs after the reporting establishment goes out of business or it is determined that the product will not be commercially marketed. Following that cutoff date, records are deleted or destroyed 10 years later, or when no longer needed for legal, research, historical, or reference purposes, whichever is the latest. If data is migrated into a new system or replaced by a successor system, records will be deleted or destroyed from the predecessor system after successful data migration has been verified.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password

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 CDER Direct application provides a web-based interface to the pharmaceutical industry that allows users to enter facility registration and product listing data as required by law and regulation. The PII collected about industry submitters — including their first and last name, work phone number, work email address, work mailing address, job title, username, and password — is collected for two primary purposes. First, this information is used to establish and maintain user accounts, enabling industry submitters to log onto the CDER Direct portal and manage their submissions. Second, the contact information is used to facilitate communication between FDA and the points of contact for regulated industry entities. Submitters provide this contact information as a practical requirement in order to communicate with FDA and to gain access to the system. The non-PII data collected about organizations — including the organization's name, mailing address, and DUNS number — is collected to identify and associate submissions with the correct regulated entity. The Drug Label and Drug Listing Data, including drug names, NDC Directory numbers, and ingredients, is collected to fulfill the legal reporting requirements under the FD&C Act and to create and archive submission packages submitted to FDA. CDER Direct contains no PII about FDA employees or Direct Contractors. FDA employees access the system via SSO and MFA, with authentication credentials maintained in Active Directory (covered in a separate privacy assessment). Therefore, no information about this category of individuals is collected into or maintained within CDER Direct itself. CDER Direct shares information with several interconnected internal FDA systems in order to carry out its submission validation and processing functions. Submissions are forwarded to the eList system for validation and subsequently to the DQCP system for processing. The system also shares information with the FDA public website (www.accessdata.fda.gov), FDA Email systems, and the CDER Electronic Drug Registration and Listing System. These interconnections are all classified as internal and operate at a Moderate security categorization, ensuring that shared information is handled with appropriate safeguards consistent with the system's own security requirements.
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://direct.fda.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

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 CDER Direct website provides a web-based interface to the pharmaceutical industry that allows users to enter facility registration and product listing data as required by law and regulation via a user-friendly data entry form. More specifically, the portal enables external users to create, submit, and manage their HL7 SPL submissions to FDA. The system supports the full lifecycle of a submission, including drafting, validation, error correction, and final acceptance. While the system is technically available to the public, it is targeted primarily at members of the pharmaceutical industry who are required by federal law to submit drug establishment registration and drug listing information to CDER. Access to CDER Direct is granted to two broad categories of users. External users, who are largely members of the pharmaceutical industry, have access to the public-facing portal to create and manage their organization's submissions. These users are restricted to accessing only their own organization's submissions and cannot view data associated with any other entity, though an organization may have more than one individual with access to its account. Internal FDA users, including a select few site administrators approved by the Business Owner, have access to the administrative application on the FDA intranet. These administrators can view user and organizational profiles and perform a limited set of privileged functions such as resetting passwords, activating or inactivating user accounts, and viewing access logs. External industry users' access CDER Direct through the public-facing production URL at https://direct.fda.gov. To gain access, new users must first register by providing their organization's DUNS number on the Create Account page. Upon submitting the registration, the system sends a confirmation email to the registered user's email address, after which the user sets their username and security answers and is assigned all administrator roles for their organization. Returning external users log in using their username and self-created password, with MFA required for authentication. Internal FDA users access the administrative application through the FDA intranet at https://dqcp.fda.gov/dqcp and authenticate via SSO. It is worth noting that while the system includes a website, the PIA confirms that none of the URLs are accessible by the general public in an unrestricted sense, as login credentials are required to access and use the system's core functionality.
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?	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- Does Not Collect PII
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 User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Job title
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	The PII of CDER Direct account holders is used to contact points of contact for industry submissions, enabling FDA to communicate with the appropriate representatives of regulated entities in the pharmaceutical industry. It is also used as access credentials to allow industry submitters to log onto the CDER Direct portal and manage their submissions. The PII contained within the submissions themselves is used for creating the submission package that is submitted to FDA as part of the drug establishment registration and drug listing process. It is also used for submission data archiving and maintenance, ensuring that a complete and accurate record of submissions is retained in accordance with the applicable NARA records retention schedule.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There are no secondary uses for which the PII maintained within CDER Direct will be used.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Applicable legal authorities governing information use and disclosure specific to the CDER Direct system and program include the following: 5 U.S.C. 301 21 U.S.C. §360(b)-(d), which establishes the legal requirement for drug establishment registration and forms the basis for the collection of Drug Establishment Registration data within CDER Direct. 21 U.S.C. §360(j), which establishes the legal requirement for drug listing and forms the basis for the collection of Drug Label and Drug Listing Data within CDER Direct.
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 Online Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB Number: 0910-0045 Expiration Date: 05/31/2029
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals who submit information through CDER Direct are notified of the collection of their PII through a posted privacy notice on the CDER Direct website. Submitters provide their contact information as a practical requirement in order to communicate with FDA and to gain access to the system. As such, by voluntarily registering for and using the CDER Direct portal, individuals are implicitly providing their consent to the collection of their PII. However, there are no opt-out procedures specific to CDER Direct. This is because 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. While the submission of PII is classified as voluntary, it is a practical necessity for any individual who wishes to access and use the CDER Direct system on behalf of their organization. If an individual does not wish to provide their PII, they may designate another authorized representative within their organization to serve as the point of contact instead.

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.	If CDER changes the collection, use, or sharing of PII data in CDER Direct, CDER will notify affected individuals by the most efficient and effective means available and appropriate to the specific change(s). This notice may include any of the following methods: Phone Call — CDER may contact affected individuals directly by phone using the work phone numbers collected as part of the account creation process, ensuring that individuals are promptly informed of any major changes to the system's collection, use, or sharing of PII. Mail Notification — CDER may notify affected individuals via standard mail using the work mailing addresses collected as part of the account creation process, providing a formal written record of any major changes to the system's privacy practices. Notice on a Website — CDER may post a notice on the CDER Direct website at https://direct.fda.gov, updating the existing posted privacy notice to reflect any major changes to the system's collection, use, or sharing of PII, ensuring that both existing and new users are informed of the current privacy practices governing the system. Email Notice — CDER may notify affected individuals via email using the work email addresses collected as part of the account creation process, providing a direct and efficient means of communicating any major changes to the system's privacy practices to all active account holders. The specific method of notification will be determined based on the nature and scope of the changes to the system's collection, use, or sharing of PII, with the goal of ensuring that all affected individuals are notified in the most efficient and effective manner possible.

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 CDER Direct have multiple avenues available for assistance, depending on their current user status (internal user or external user). Individuals may contact FDA offices via email, phone, and standard mail, all of which are listed on fda.gov and the FDA intranet. Specifically, the following FDA offices are available to assist individuals with their concerns: FDA Privacy Office — The FDA Privacy Office serves as the primary point of contact for individuals who have concerns about the inappropriate collection, use, or disclosure of their PII within any FDA system, including CDER Direct. Employee Resource and Information Center (ERIC) — ERIC is available to assist internal users who have concerns about the handling of their PII within FDA systems and can provide guidance on the appropriate steps to take to resolve those concerns. Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) — The CIOCC is available to assist internal users who have concerns about potential security incidents or breaches that may have resulted in the inappropriate obtaining, use, or disclosure of their PII within CDER Direct or any other FDA system. In the event of a suspected incident or data breach, FDA personnel must rapidly report that without delay to FDA's 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.	Accuracy of PII within CDER Direct is primarily ensured through individual review at the time of reporting. Since individuals voluntarily provide their own PII, they are responsible for ensuring that the information they submit is accurate. FDA personnel may correct or update their own information as needed, ensuring that the PII maintained within the system remains current and accurate. Additionally, CDER Direct support staff performs annual reviews to evaluate user access, providing an additional layer of oversight to help ensure the accuracy of PII maintained within the system. The relevancy of PII maintained within CDER Direct is supported through the design of the system itself, which is configured 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 through role-based access controls, ensuring that only relevant and necessary PII is collected and maintained within the system. The integrity of PII maintained within CDER Direct is protected by privacy and security controls selected and implemented in the course of providing the system with an Authority to Operate (ATO). These 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. Additionally, technical safeguards ensure that PII entered via the system is immediately pulled through the web-based systems into internal systems not connected to the web, removing it from the public site and preventing it from being accessible to others submitting information via the system or fda.gov. The availability of PII maintained within CDER Direct is similarly protected by the privacy and security controls implemented as part of the system's ATO process. These controls are selected based on NIST guidance and are appropriate to the system's Moderate security categorization, ensuring that PII remains available to authorized users as needed to carry out their regulatory reporting obligations and system administration functions. Physical controls, including guards, locked facility doors, and climate controls at the FDA facilities where the system's servers are located, further support the availability of PII by protecting the underlying infrastructure from physical threats.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators 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 (Industry Submitters) — External industry users, who are members of the pharmaceutical industry, have access to the PII associated with their own submissions and account information. These users are restricted by their accounts to only being able to access PII created from their own submissions and cannot view data associated with any other entity. An organization may have more than one individual with access to its account, but those individuals will not have access to accounts associated with any other entity. Administrators — CDER Direct Administrators, which include a select few FDA employees appointed by the business sponsor (the Drug Registration and Listing Office), have access to all PII within the system in order to perform system operation monitoring, maintenance, and user assistance functions. Administrative user access is controlled by the business sponsor and is granted only to those whose confirmed role requires such access. Contractors — A limited number of HHS/Operating Division (OpDiv) Direct Contractors serve as application administrators for application operational support and have access to PII within the system as necessary to perform their job functions. Contracts with these contractors include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. It is worth noting that while FDA employees access the system via SSO and MFA, the PIA confirms that CDER Direct contains no PII about FDA employees or Direct Contractors. Therefore, the PII accessible to administrators and contractors pertains solely to the industry submitters and their associated organizational information.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only FDA employees and Direct Contractors with a CDER Direct Administrator role can access all PII information within CDER Direct. All administrative users must be appointed by the business sponsor, the Drug Registration and Listing Office, to be granted appropriate access based on their confirmed role. This ensures that administrative access to PII is limited to only those individuals whose job functions require such access, in accordance with the Need to Know and Minimum Necessary principles. Users from industry are granted access to their own submissions when signing up for a CDER Direct account and are restricted to only being able to access PII created from their own submissions. An industry entity may have more than one individual with access to the entity's account; however, those individuals will not have access to accounts associated with any other entity. Industry users can create accounts on behalf of their organization only and may expand that access to their own sub-organizations, but account settings and technical controls ensure that industry submitters can only see their own account information.

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.	Industry submitters are restricted by their accounts to only being able to access PII created from their own submissions. Industry users can create accounts on behalf of their organization only and may expand that access to their own sub-organizations. Account settings and technical controls ensure that industry submitters can only see their own account information and cannot access PII associated with any other entity or organization. This ensures that external users are limited to accessing only the minimum amount of PII necessary to fulfill their regulatory reporting obligations under the FD&C Act. CDER Direct Administrators, including both FDA employees and Direct Contractors with an administrator role, are able to access all PII within the system in order to perform their job functions. However, administrative user access is controlled by the business sponsor, the Drug Registration and Listing Office, and is limited to a select few FDA employees and Direct Contractors whose confirmed roles require such access. This ensures that administrative access to PII is granted only to those individuals whose job functions necessitate it, in accordance with the Need to Know and Minimum Necessary principles. The system implements several technical safeguards to ensure that PII is protected and accessible only to those who need it. PII entered via the CDER Direct web-based portal is immediately pulled through into internal systems not connected to the web, removing it from the public site and preventing it from being accessible to others submitting information via the system or fda.gov. Role-based access controls are implemented at the individual level, ensuring that access to PII is granted and restricted based on each user's confirmed role and associated job functions. Additionally, the system employs SSO with MFA for internal FDA users and username and password authentication with MFA for external industry users, providing an additional layer of technical security to ensure that only authorized individuals are able to access the system and the PII maintained within it.

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, including system owners, managers, operators, contractors, and program managers, are required to complete 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. This ensures that all personnel are aware of their legal obligations and responsibilities with respect to the protection of PII and other sensitive information collected and maintained within CDER Direct. The FDA Office of Digital Transformation (ODT) verifies that training has been successfully completed by all system users, providing an additional layer of oversight to ensure that all personnel are current with their mandatory training requirements before being granted access to the system and the PII maintained within it.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to the annual mandatory computer security and privacy awareness training required of all FDA system users, personnel with access to CDER Direct receive two additional forms of training specific to their roles and responsibilities within the system. First, personnel are trained on the use of the CDER Direct system itself, ensuring that all users are familiar with the system's functionality and the appropriate procedures for entering, managing, and submitting data within the system. As part of this system-specific training, all personnel are required to review and acknowledge the Rules of Behavior for CDER Direct, ensuring that they are aware of their responsibilities for protecting the information being collected and maintained within the system and the consequences of failing to adhere to those responsibilities. Second, additional role-based training on privacy is available to all personnel via FDA's Privacy Office, providing more targeted guidance on privacy responsibilities and best practices specific to each individual's role and job functions within the system.

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).	Industry submissions containing PII are archived in the system following an FDA General Retention Schedule (GRS). Records are retained in CDER Direct under the schedule tracked by NARA Approved Citation N1-88-07-2, under FDA File Codes 7220/7222, which covers Compliance (Agency-Wide); Registration and Listing Systems; and Database Records. Under this retention schedule, records are maintained until a "cutoff date," which occurs under one of the following two conditions: after the reporting establishment goes out of business, or when it is determined that the product will not be commercially marketed. Following the cutoff date, records will be deleted or destroyed 10 years later, or when no longer needed for legal, research, historical, or reference purposes, whichever is the latest. This ensures that records are retained for as long as they may be needed for legitimate legal, research, historical, or reference purposes, while also ensuring that they are destroyed in a timely manner once those purposes have been fulfilled. In cases where data are migrated into a new system or replaced by a successor system, records will be deleted or destroyed from the predecessor system after the successful migration of data to the new or successor system has been verified. This ensures that duplicate records are not retained in the predecessor system following a successful data migration, in accordance with applicable NARA records retention requirements and FDA records management policies.
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 implemented within CDER Direct include several key measures to ensure the protection of PII. All system users are required to complete annual mandatory computer security and privacy awareness training, which covers 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. System documentation advises personnel on the proper use of the system, and the Need to Know and Minimum Necessary principles are implemented when awarding access to ensure that individuals are only granted access to the PII necessary to perform their job functions. All personnel are required to review and acknowledge the Rules of Behavior for CDER Direct, and additional role-based training on privacy is available via FDA's Privacy Office. Contracts with HHS/OpDiv Direct Contractors include FAR and other appropriate clauses ensuring adherence to privacy provisions and practices, providing an additional layer of administrative oversight for contractor access to PII within the system. Technical safeguards implemented within CDER Direct include several key measures to protect PII from unauthorized access and disclosure. PII

entered via the CDER Direct web-based portal is immediately pulled through into internal systems not connected to the web, removing it from the public site and ensuring that it is not accessible to others submitting information via the system or fda.gov. Role-based access controls are implemented at the individual level, ensuring that access to PII is granted and restricted based on each user's confirmed role and associated job functions. Industry submitters are restricted by their accounts to only being able to access PII created from their own submissions, while CDER Direct Administrators are limited to a select few FDA employees and Direct Contractors whose confirmed roles require broader access to PII within the system. The system employs SSO with MFA for internal FDA users and username and password authentication with MFA for external industry users, providing an additional layer of technical security to ensure that only authorized individuals are able to access the system and the PII maintained within it. Additionally, other appropriate controls have been selected from NIST's Special Publication (SP) 800-53, as determined using FIPS 199, to ensure that the system's technical safeguards are appropriate to its Moderate security categorization.

Physical safeguards implemented within CDER Direct include measures to protect the underlying infrastructure of the system from physical threats. All system servers are located at FDA facilities, specifically the FDA Data Center (ADC), and are protected by a combination of physical security measures including guards, locked facility doors, and climate controls. These physical controls ensure that the servers hosting CDER Direct and the PII maintained within it are protected from unauthorized physical access, environmental hazards, and other physical threats that could compromise the integrity, availability, or confidentiality of the system and its data.

Appropriate controls have been selected from the NIST’s Special Publication 800-53 as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/3/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/3/2026
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. 6/3/2026 Note the Archer error associated with question General 03: "Does the system have or is it covered by a Security Authorization to Operate (ATO)?" The FDA instance of Archer is automatically entering the answer "No" which is incorrect. At this time, we are unable to update Archer to reflect the correct answer "Yes." The ATO date is11/18/2025. The FDA Archer Team is aware of this occurrence and is working on a solution	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/8/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 6/8/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	5

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/8/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/8/2026 2:39 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	6/8/2026	6/8/2026 Per FDA's Email, PIA is attached.	CDER Direct SOP approved 6.3.26.pdf