PTA / PIA: FDA - EA - QTR2 - 2026 - FDA5270067

Created Date: 5/11/2026 10:20 AM Last Updated: 5/29/2026 6:17 PM

General Information

PTA / PIA Name:	FDA - EA - QTR2 - 2026 - FDA5270067	**PTA / PIA ID:**	4473986
Component Name:	FDA - OC eArrive	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	25
Submitter:		**Submit Date:**	5/4/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
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?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	10/6/2025
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	Robin Bock
PTA 01A:	POC Title and Organization	Office of Operations (OO) Branch Chief, Human Resources Systems Records and Management
PTA 01B:	POC Email Address	Robin.Bock@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-9967
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.	Since this Privacy Threshold Analysis/ (PTA) Privacy Impact Assessment (PIA) was last approved, FDA made the following changes: Changed system component name to eArrive (formerly Automated Employee Entrance Process); Fixed bug to allow OC Automated Employee Entrance Process (eArrive) notification emails to be sent to external (outside FDA) email addresses. Changed a few email inbox addresses for notifications; Changed Cybersecurity Awareness Training (CSAT) notification template, but then later removed automated sending of CSAT notification; Relabeling of "Gender" as "Sex" in notifications; Updated some items for 508 compliances; Removed the automation of assignment of eArrive records based on the center to allow for the assignment of eArrive records where the employee type code is "Commissioned Corp" to flow to the Security application queue; Updated error messages and success messages; and Updated Office of Security & Emergency Management (OSEM) Basic User and System Admin Role.
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) Administrative Applications (Admin Apps) initiative was designed to meet mandated tracking requirements for administrative functions that take place throughout the agency, The initiative provides FDA personnel with a single system with shared functionalities for cost-effective application development, a common user-experience, and improved maintenance through standardized interface, features, and components. The subject of this assessment is OC eArrive, a component of the larger Administrative Applications system boundary. OC eArrive (formerly referred to as Automated Employee Entrance Process) is a web-based system used by FDA to standardize onboarding procedures for all new hires. The system is designed to ensure the completion of all necessary onboarding processes prior to a new hire's initial reporting date at the FDA. OC eArrive's capabilities include issuance of Personal Identity Validation (PIV) cards (FDA badge); establishing an FDA network account; creating an FDA email address; and providing an opportunity to complete information technology (IT) security awareness training. OC eArrive is used for on-boarding permanent

employees, direct contractors, and non-FDA government employees. The system component serves as a critical gateway in the personnel entry process, as individuals cannot proceed through the security process or receive network access without first being processed through OC eArrive. This makes it an essential component of FDA's personnel management infrastructure and a mandatory step in bringing new personnel into the agency.

The application functions as a front-end entry point to the broader Enterprise Administrative Support Environment (EASE), another Admin Apps component (and subject of its own assessment) that aggregates personnel data from the Department of Health and Human Services (HHS) Human Resources system and Commissioned Corps (CC) Personnel applications, as well as non-employee data entered directly into EASE. By serving as this front-end interface, OC eArrive facilitates the initial data collection and processing necessary to establish new personnel in FDA's administrative systems. The system ensures that all required information is captured at the beginning of an individual's employment with FDA, creating a foundation for subsequent personnel management activities.

The system's primary function, to initiate and track the on-boarding workflow for new FDA personnel, ensures that all necessary steps are completed before individuals receive security clearances and network access. This includes collecting essential personnel information, coordinating required security training, and establishing the individual's record in EASE, which then becomes the central repository for their personnel data throughout their time with the agency.

Access to OC eArrive requires users to authenticate through FDA's internal network using their FDA issued PIV cards and Single Sign-On (SSO) authentication via Active Directory (covered in separate assessment). Access is restricted to users connecting from within the FDA network or through a secure Virtual Private Network (VPN) connection. The system is not accessible via a public uniform resource locator (URL) and cannot be reached from the open internet. Access controls are enforced based on user roles and permissions, ensuring that even among authorized FDA employees, users can only access the functions and data necessary for their specific job responsibilities. Multi-factor authentication is required as part of FDA's information security protocols for systems handling sensitive personnel information.

It is important to note that while OC eArrive interfaces with HHS systems through its connection to EASE, the system's primary purpose is supporting FDA's internal on-boarding processes rather than directly supporting HHS operations.

		The system ensures that new FDA permanent employees, direct contractors, and non-FDA government employees are properly processed, vetted, and granted appropriate access to FDA resources in accordance with federal security and agency personnel management requirements. Through this function, OC eArrive plays a critical role in maintaining the security and integrity of FDA's workforce by ensuring that only properly vetted and authorized individuals gain access to agency systems and facilities.
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.	OC eArrive collects, maintains and shares Personally Identifiable Information (PII) and non-PII associated with the FDA's new hire on-boarding process. As a front-end entry point to EASE, OC eArrive captures essential data needed to establish new employees, contractors, and non-FDA government employees in FDA's administrative systems and enable their access to agency resources. OC eArrive collects, maintains, and shares the following professional and personal contact information PII about FDA permanent employees, direct contractors, and non-FDA government employees entering the agency (selected job applicants who have not completed the onboarding process): (a) Social Security number (SSN), (b) first and last name, (c) email address (personal and business), (d) phone number (personal and business), (e) date of birth (DOB), (f) mailing address (personal and business), (g) training certificates and employment status/history/job titles, (h) employee identification number, (i) security clearances (including biometric data in the form of fingerprints), (j) background check data, (k) passport information (includes photographic identifier and citizenship status), (l) driver's license, (m) education records, and (n) other forms of identification cards . PII is used to conduct administrative human resources related functions, including tracking employees and direct contractors and ensuring they are satisfying privacy and security requirements that are conditions of their employment, and completing onboarding activities. PII is also used for communication purposes with incoming personnel throughout the on-boarding process, coordinating required activities such as security training and background checks, and ensuring all parties involved in bringing new personnel into the organization can reach the individual during the entry process. Specific unique identifiers (SSN, HHS employee identification numbers, driver's license, passport information, and other forms of identification) are used to accurately track individuals through the on-boarding process and ensure that security clearances, network access provisioning, and other entry tasks are associated with the correct personnel records. The system also maintains

		dates of employment or contract work to establish timelines for on-boarding activities and determine when individuals should receive access to FDA systems and facilities. As individuals cannot proceed through the security process or receive network access without being processed through OC eArrive, the system maintains information related to security clearances (biometric data collected includes fingerprints), background check status, and required security training completion. Data subjects have access to OC eArrive in order to take the required security training prior to having access to FDA systems. This ensures that all incoming personnel complete mandatory security requirements before being granted access to sensitive information or agency resources. Beyond the specific categories mentioned above, the system stores any information sent from personnel systems that would be relevant to internal human resources functions. This broad category encompasses data necessary for conducting administrative on-boarding activities and ensuring incoming employees and direct contractors satisfy privacy and security requirements that are conditions of their employment or contract work with the agency. Both PII and non-PII are maintained in OC eArrive in accordance with National Archives and Records Administration (NARA) record schedules. PII is used to retrieve records from the system.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Lightweight Directory Access Protocol (LDAP)/Active Directory (AD)
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.	OC eArrive is used by FDA to standardize onboarding procedures for all new hires. The system is designed to ensure the completion of all necessary onboarding processes prior to a new hire's initial reporting date at the FDA. Capabilities include issuance of new hire PIV cards; establishing FDA network user accounts; creating FDA email addresses; and completing IT security awareness training before official start date. PII is also used to conduct other administrative human resources related functions, such as tracking fulfillment of employee and direct contractor privacy and security requirements that are conditions of their employment. OC eArrive also collects, maintains, and shares information to ensure that all incoming employees, contractors, and non-FDA government employees complete necessary security and administrative processes before gaining access to agency resources. Each data category collected,

maintained, and shared serves specific purposes related to establishing personnel records, verifying identities, ensuring security compliance, and facilitating the transition of new personnel into the organization.

OC eArrive collects the following PII about incoming employees, direct contractors, and non-FDA government employees entering the agency: (a) Social Security number (SSN), (b) first and last name, (c) email address (personal and business), (d) phone number (personal and business), (e) date of birth (DOB), (f) mailing address (personal and business), (g) training certificates and employment status/history/job titles, (h) employee identification number, (i) security clearances (including biometric data in the form of fingerprints), (j) background check data, (k) passport information (includes photographic identifier and citizenship status), (l) driver's license, (m) education records, and (n) other forms of identification cards .

The system collects professional and personal contact information including name, email address, phone numbers, physical addresses, and email addresses for FDA employees, direct contractors, and non-FDA government employees who are entering the agency. This contact information is essential for communicating with incoming personnel throughout the on-boarding process and coordinating the various activities required before an individual can begin work at the agency. The system uses this data to send notifications about required security training, schedule background check appointments, coordinate badge issuance, arrange for equipment provisioning, and ensure all parties involved in the on-boarding process can reach the individual. Email addresses enable automated notifications about pending tasks and deadlines for completing on-boarding requirements, while phone numbers and physical addresses support follow-up communications regarding orientation sessions, security clearance status, and other critical on-boarding activities. Without accurate contact information, the agency would be unable to effectively guide new personnel through the complex entry process or ensure timely completion of all mandatory requirements. This information is shared with EASE to establish the individual's permanent personnel record and may be shared with security offices, human resources systems, and facilities management to coordinate the various aspects of onboarding new personnel into the organization.

OC eArrive collects SSN, HHS employee identification and dates of employment or contract work for FDA employees and direct contractors entering the agency. Passports, driver's license and identification cards will be used to verify identities as well. These unique identifiers are critical for accurately tracking individuals through the on-

boarding process and ensuring that security clearances, network access provisioning, and other entry tasks are associated with the correct personnel records. SSN, HHS employee identification, passport, and/or driver's license prevent confusion between individuals with similar names and ensure that background checks, security training completion, and access grants are applied to the appropriate person. These identifiers are essential for conducting background investigations, verifying employment eligibility, establishing payroll records, and creating unique user accounts in FDA systems. Dates of employment or contract work establish timelines for on-boarding activities, determine when individuals should receive access to FDA systems and facilities, and ensure compliance with start date requirements. This information is shared with EASE to create the individual's central personnel record, with payroll systems to establish compensation, with benefits administration systems to enroll new employees in appropriate programs, and with background investigation services to verify identity and conduct security clearances. The precision provided by these unique identifiers is essential for maintaining the integrity of personnel records from the moment an individual enters the agency and preventing identity-related errors that could compromise security or administrative processes.

The system collects records related to security clearances, background check status, and required security training completion for FDA employees, direct contractors, and non-FDA government employees entering the agency to ensure security and agency requirements have been met before a new hire's official start date with FDA. Individuals cannot proceed through the security process or receive network access without first being processed through OC eArrive, and making this a critical control point for agency security. The system maintains information about background check initiation and completion status to ensure that all incoming personnel undergo appropriate vetting before receiving access to sensitive information or facilities. Security training records document that new personnel have completed mandatory training on information security, privacy protection, and other security-related topics that are prerequisites for system access. Data subjects have access to OC eArrive specifically to take the required security training prior to having access to FDA systems, ensuring they understand their security responsibilities before being granted access to agency resources. This information is shared with security offices to coordinate background investigations and clearance determinations, with network administration systems to trigger account creation only after security requirements are met, with Active Directory to provision appropriate access levels based on clearance status, and with training management systems to maintain comprehensive records of completed security training. The

		collection and maintenance of this information protects the agency by ensuring that only properly vetted and trained individuals gain access to FDA systems and facilities, thereby reducing the risk of security incidents involving new personnel who may not yet understand agency 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://adminapps.fda.gov/EA
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The OC eArrive website serves as the on-boarding application for both employees and non-employees entering the FDA. It functions as a mandatory gateway system - individuals cannot proceed through the security process or receive network access without first being processed through OC eArrive. The application serves as a front-end entry point to EASE, which manages broader personnel data across the agency. Access to OC eArrive requires users to authenticate through FDA's internal network using their FDA PIV cards and SSO authentication via Active Directory. Access is restricted to FDA authorized users connecting from within the FDA network or through a secure VPN connection. The system is not accessible via a public URL and cannot be reached from the open internet. Access controls are enforced based on user roles and permissions, ensuring that even among authorized FDA employees, users can only access the functions and data necessary for their specific job responsibilities. Multi-factor authentication is required as part of FDA's information security protocols for systems handling sensitive personnel information.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Driver's License Number Passport Number Employee ID Number Biographical Information Name Date of Birth Certificates (e.g., training certificates) Education Records Employment Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Biometrics/Distinguishing Features Biometric Identifiers (e.g., fingerprints, retina scans, DNA samples) Photographic Identifiers Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Security clearance (includes biometrics-fingerprinting); Background Checks, HHS employee identification numbers, other identification card(s), and job title (as included in employee status/history). Any other information relevant to inquiries concerning individuals' identity. Passports and Driver's License (includes photographic identifier) are used for identification purposes. The collected contact information can be either personal or professional contact information.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors 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?	OC eArrive uses PII to facilitate and document the on-boarding process while ensuring compliance with employment conditions, particularly privacy and security requirements necessary to establish access and credentials for new personnel to function within the FDA environment, as well as communication purposes.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The FDA makes no secondary use of the PII.

PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	SSN is used to identify individuals when required by law (or when for any reasons identification is not otherwise possible). For example, use of an individual's SSN is required to conduct certain security functions, such as background checks.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	Use of SSN is supported by Executive Order 9397, as amended.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Use of SSN is supported by Executive Order 9397, as amended. Personnel security functions required by the Security application as well as some functions of eArrive and eDepart are supported by Homeland Security Presidential Directive (HSPD) 12, which requires in part that "the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification" to "enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy." General authority for implementing regulations for the usual and necessary infrastructure of running an organization is provided to agencies by 5 U.S.C 301. These systems enable fundamental business practices such as hiring, separating departing employees, providing employees access to resources, and protecting infrastructure. These systems support the necessary function of identifying, evaluating, and employing staff with appropriate knowledge, skills and abilities, an activity authorized generally by 5 U.S.C. Sec. 3101, "General authority to employ: Each Executive agency, military department, and the government of the District of Columbia may employ such number of employees of the various classes recognized by chapter 51 of this title as Congress may appropriate for from year to year." Other authorities related to the use and disclosure of employment-related information can be found in 5 U.S.C. Part III.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The following PII data elements are used to retrieve records from OC eArrive: Name, Date of Birth, E-Mail Address, Phone Number and Employment Status.
PIA 29B:	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.	OPM GOVT-1 (General Personnel Records) SORN 09-90-0777, Facility and Resource Access Control Records

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Phone Email Online Government Sources Within the OPDIV Non-Government Sources Members of the Public
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 No. 3209 0001- Form OGE 278e (ethics form). Expiration date is 8/31/2027 OMB No. 3209-0006-Form OGE 450 (Confidential Financial Disclosure Report). Expiration date is 8/31/2027
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.	Employment at FDA is voluntary; however, the information is necessary to appropriately clear employees and contractors; award them appropriate access; and conduct necessary functions such as tracking the provision of mandatory training, track computers and other equipment assigned, issue PIV badges, and others. Should an individual choose not to provide their PII they cannot be considered for employment with FDA.
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 the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on an FDA website, email notice to the individuals, inclusion in newsletters, or information provided to supervisors with instructions to further inform staff. However, no such changes that would affect the rights or interests of the individuals are anticipated. Individuals have many other options available to address their concerns. They may work through their supervisors, human resources officials, the FDA Privacy Office, information system security officers, the information system owner, the Computer Security Incident Response Team, or the employee help line to address any concerns about inaccuracies or incidents.

PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have many avenues available for assistance. External users may contact FDA offices, including the Privacy Office, and other agency offices, via email, phone, and standard mail avenues (all listed on fda.gov). Internal FDA users may contact FDA offices, including the Privacy Office, the Employee Resource, and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone, and standard mail avenues (all listed on fda.gov and the FDA intranet). HHS and FDA policy obligates personnel to report suspected breaches. Within FDA, all reports of suspected and confirmed breaches must be reported to the CIOCC.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by privacy and security controls selected and implemented while 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 National Institute of Standards and Technology (NIST's) Federal Information Processing Standards (FIPS) 199. System administrators perform annual reviews to evaluate user access.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: "Users" are FDA employees that have access to the various applications to perform FDA administrative functions, not the data subjects themselves. Require full access to systems to conduct activities related to onboarding and hiring, providing access to systems and networks, and other administrative activities. Note that "users" may include subject individuals, supervisors, or business function administrators. Administrators: Administrators may be application administrators who require access to conduct business functions, or application administrators who require access to create and manage user accounts for specific applications. Developers: Developers will not normally have access to PII but may in the course of maintaining the systems or providing technical assistance. Direct Contractors: Some developers may be direct contractors and will have access under the same circumstances as developers.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	For all applications, administrative access is granted by existing system administrators. New users seek administrative access when assigned duties requiring this access. Employees then coordinate with applications administrators who in turn inform employees of how to log on and what actions must be taken. The user's supervisor uses an account creation form to specify the minimum information system access that is required for the user to complete required tasks.
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.	Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his or her job.
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 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). The FDA Office of Digital Transformation (ODT) verifies that training has been successfully completed.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	A user manual is available that walks the user through each step and functionality of many of these applications. For example, manuals for eArrive and eDepart are freely available and conspicuously linked on the FDA Intranet. These provide guidance for subject individuals as well as administrators that create accounts. The other applications have documentation as well and are posted on the FDA Intranet. All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the agency's Privacy Office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.
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).	Applications operating under the Admin Apps system boundary are maintained under General Records Schedule (GRS) 3.2, Information Systems Security Records, Item 030, System Access Records. This schedule includes “records created as part of the user identification and authorization process to gain access to systems.” Disposition for these files is temporary, and the files may be destroyed/deleted when business use ceases. If the application owner determines that an application requires special accountability, retention may be six years after the password is altered or the user account is terminated, and longer retention is authorized if required for business use. (The exception here would be the EASE component which is maintained by FDA schedule 9110 File Code series, File Codes 9111 through 9117 inclusive. 9111 covers Inputs (Core and Other Data)). The application electronically manages the lifecycle of documents as it relates to the agency National Archives and Records Administration (NARA) records retention schedule. Retention times for individual forms vary based on the specific form type and are maintained as follows, with forms to be destroyed after the retention period unless there is an ongoing use, such as when needed in an ongoing investigation: The application electronically manages the lifecycle of documents as it relates to the agency National Archives and Records Administration (NARA) records retention schedule. Retention times for individual forms vary based on the specific form type and are maintained as follows, with forms to be destroyed after the retention period unless there is an ongoing use, such as when needed in an ongoing investigation: FDA 2096 follows Schedule 9461 with a six-year retention period; FDA 2097 follows Schedule 9412 with a six-year retention period; Office of Government Ethics (OGE) 450 follows Schedule 9422a with a one-year retention period if

		not confirmed for a position, or Schedule 9422b with a six-year retention period for all others; OGE 450A follows Schedule 9422b with a six-year retention period; OGE 278 follows Schedule 9421a with a one-year retention period if not confirmed for a position, or Schedule 9421b with a six-year retention period for all others; OGE 278T follows Schedule 9421b with a six-year retention period; HHS 717-2 follows Schedule 9430 with a six-year retention period; HHS 520 follows Schedule 9470 with a six-year retention period; HHS 521 follows Schedule 9451 with a three-year retention period; and FDA 3539 follows Schedule 9411 with a three-year retention period.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative Safeguards include training and awareness provided for all users; system manuals that advise on proper use of the system; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include that PII entered via these systems is immediately pulled through the web-based systems into the systems that are internal and not connected to the web and not accessible to others submitting information via these systems or fda.gov. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. 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:**	5/4/2026
Privacy Analyst Review Comments:	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 is 10/6/2025. The FDA Archer Team is aware of this occurrence and is working on a solution.	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/11/2026
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. 5/11/2026	**# of Days - SOP Review:**	7

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/21/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/21/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	10

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 2:58 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	5/11/2026	5/11/2026 Per FDA's Email: The PIA is experiencing an Archer error with Question #3 of the general information section. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” o The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. The ATO date is 10/6/2025. o At this time, we are unable to update Archer to reflect the correct answer “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	OC eArrive (AKA _Automated Employee Entrance Process_).pdf OC eARRIVE SOP approved 5.11.26.pdf
PTA 02A	DORKENOO, PHILOMINA	5/15/2026	.	