PTA / PIA: FDA - FOIAXPress - QTR3 - 2025 - FDA4949737

Created Date: 7/30/2025 4:45 PM Last Updated: 8/5/2025 12:43 PM

General Information

PTA / PIA Name:	FDA - FOIAXPress - QTR3 - 2025 - FDA4949737	**PTA / PIA ID:**	3574902
Component Name:	FDA - CDRH FOIAXPress	**ATO Boundary Name:**	CDRH Reporting and Collection Tools
Overall Status:	Complete	**# of Days - Open:**	6
Submitter:		**Submit Date:**	7/30/2025
Next Assessment Date:	08/04/2028	**Expiration Date:**	8/4/2028
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.	1/23/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	POC Name: Candace Boston
PTA 01A:	POC Title and Organization	Title: Director, Division of Information Disclosure
PTA 01B:	POC Email Address	candance.boston@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-3736
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.	FDA has made no changes to this system since the last Privacy Threshold Analysis/Privacy Impact Assessment 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 purpose of the Freedom of Information Act Xpress system (FOIAXpress) is to enable the Center for Devices and Radiological Health (CDRH) Division of Information Disclosure (DID) and its Direct Contractors to more efficiently manage the processing of FOIA requests made to the Agency under FOIA and the Privacy Act (PA). The system securely stores, processes (redacts content to prevent prohibited disclosure of content by obscuring it) and transmits records responsive to requests. It generates associated correspondence as well as internal and public reports in a manner that complies with statutory and Department of Justice (DOJ) requirements and best practices. The CDRH FOIA team implementation of FOIAXpress replaces a manual system that does not provide adequate tracking and reporting capability. FOIAXpress provides more robust storage, templates, online features, support for compliance with section 508 of the Rehabilitation Act (making information accessible to persons with disabilities), and request processing/tracking tools. Information is imported into FOIAXpress through a separate system known as AINS Inc. (AINS), a cloud-based software which provides information directly to FOIAXpress. AINS is considered a source system for FOIAXpress and is the subject of a separate FDA Privacy Impact Assessment. Note also that requests submitted to FDA through the FDA.gov FOIA submission page are taken in through FDA's Agency Information Management System (AIMS) not FOIAXpress. FDA has evaluated AIMS in a separate Privacy Impact Assessment. FOIAXpress does not have public facing elements and does not receive requests directly from the submitting individual or entity.

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 personally identifiable information (PII) in the system is primarily about members of the public who submit FOIA record requests to FDA/CDRH. Current and former employees who submit FOIA requests do so in their personal capacity (not a work duty). Other PII subjects include CDRH analysts assigned to requests and individuals identified in records gathered in response to requests. CDRH FOIAXpress collects the following PII: (a) the requester's name; (b) the requester's home and/or personal mailing and email address, as well as phone numbers; (c) the requester's organization and business name; (d) the name, of the FDA FOIA analyst assigned to the case, and (e) other PII provided in correspondence with the requester and within agency records gathered in response to a FOIA request can include social security number which is collected using the FDA Certification of Identity 3975 form to confirm the identity of the requestor submitting a FOIA request to the FDA. Medical notes, date of birth, medical records, financial account information, legal documents, certificates, taxpayer ID, device identifiers, employment status, and biometric identifiers are other PII that can be included. Occasionally a requester includes additional PII about other individuals in the substance of his/her record request (e.g., a request for memoranda written by a specific named individual). The CDRH FOIA analysts redact any personal information and identifiers not disclosable under FOIA and trade secret information before entering in FOIAXpress. FDA/CDRH retains the PII for up to six years after a case is closed. CDRH does not share the PII in FOIAXpress with any other system or organization. CDRH FOIAXpress collects the following non-PII: (a) summary of the request history; (b) the number of pages, or portions of pages, of responsive records located, released or withheld; (c) the agency's decision on any appeal issues, (d) internal notes and comments; and (e) a notice of appeal rights. In addition, FOIAXpress may receive a FOIA request accompanied by a full or partially completed FDA Certification of Identity form 3975. This form is used by members of the public to verify their identity when submitting a FOIA request to the FDA. The 3975 form collects the following PII: (a) full name of requester; (b) Social Security number (SSN); (c) current mailing address; and (d) date of birth. Also, the form collects the following non-PII: (a) citizenship status and (b) place of birth. The users of FOIAXpress who have access to the PII are limited to members of CDRH's Division of Information Disclosure (DID) FOIA staff, including Direct Contractors.
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.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address HHS 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.	FOIAXpress is an all-inclusive system that provides the FDA and CDRH FOIA Office with all tracking, storage, processing, communication, management, and reporting tools required to administer the Agency's Freedom of Information Act (FOIA) program in accordance with government best practices. The information collected in FOIAXPress is received directly from the FDA's Division of Freedom of Information (DFOI) and the Agency Information Management System (AIMS) system which is the system that initially receives record requests from members of the public and external entities. The AIMS system is covered in a separate privacy assessment. CDRH FOIA's permanent staff and Direct Contractors access AIMS and upload CDRH -related requests from AIMS to FOIAXpress. The users of the system consist of FDA employees and Direct Contractors. All users access system using a personal identity verification (PIV) card and single sign-on (SSO) process with multi-factor authentication. CDRH FOIAXpress collects the following PII: (a) the requester's name; (b) the requester's work, home and/or other personal mailing and email address as well as phone numbers; (c) the requester's organization and business name; and (d) the name of the FDA FOIA analyst assigned to the case. Requesters may also include PII in the wording of their request. In addition, FDA Certification of Identity form 3975 also may collect PII in the form of the full name of requester, Social Security number, current mailing address, and date of birth. Also collected is non-PII in the form of citizenship status as well as place of birth. The FOIA analysts are instructed to redact any PII and trade secret information before entering in FOIAXpress. The PII maintained in the system is retained for a period of six years and not shared with any other system or organization. The FDA/CDRH DID personnel use PII to retrieve FOIA and Privacy Act requests. These records can be retrieved using the requester's name. The PII used to retrieve records in the system relates to people who submit FOIA requests. Submitters include members of the general public as well as business partners including staff at other federal agencies and state/local liaisons. The PII about business partners is collected only if there is a referral from another agency that includes PII in the points of contacts and notes sections of the system documentation.
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://fdacdrh-prod.efoia-host.com/FOIAXpress/UserHome.aspx
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.	CDRH FOIAXpress (FOIAXPress) is an internal-facing application used by CDRH to manage and respond to Freedom of Information Act (FOIA) requests. CDRH FOIAXpress enables the CDRH FOIA Office and its Direct Contractors to more efficiently receive, track, and respond to records requests and appeals made to the Agency under the FOIA and the Privacy Act. FOIAXPress SaaS is Security Assertion Markup Language (SAML) enabled internal website that is only accessible by FDA Employees and Direct Contractors using a personal identity verification (PIV) card and single sign-on (SSO) process with multi-factor authentication. Users may also login using user credentials (name, email address (business), and password).
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 Financial Account Information (e.g., account numbers, credit card numbers) Device Identifiers Biographical Information Name Date of Birth Certificates (e.g., training certificates) 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) Medical Information Medical Records Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Name and email address of FDA employees and Direct Contractors are considered business professional context PII. For requestors - SSNs are collected using the FDA Certification of Identity 3975 form to confirm the identity of the requestor submitting a FOIA request to the FDA. This form is used by members of the public to verify their identity when submitting a FOIA request to the FDA. The 3975 form collects the following PII: (a) full name of requester; (b) Social Security number (SSN); (c) current mailing address; and (d) date of birth. Also, the form collects the following non-PII: (a) citizenship status and (b) place of birth.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	5,000 – 9,999

PIA 25:	For what primary purpose is the PII used?	The primary purposes for which PII in CDRH FOIAXpress is used is to manage record requests: (a) document and analyze requests received from individual requesters; (b) locate responsive records, verify the identity of individual requesters; (c) contact requesters; (d) locate cases and related requests in the system (same requester, similar records requested); (e) process responsive records containing PII; (f) maintain clean, marked and redacted versions of the processed records; (g) document responses to requests and fee issues; and (h) generate status reports.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There are no secondary uses.
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.	SSNs are collected using the FDA Certification of Identity 3975 form to confirm the identity of the requestor submitting a FOIA request to the FDA.
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.	Executive Order (E.O.) 9397 as amended by E.O. 13478. SSN is necessary for purposes of verifying identity and distinguishing between individuals to ensure responses to record requests are accurate, permitted by law, and provided to the correct individual and no one else.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	44 U.S.C. 3301 (definition of records), 5 U.S.C. 301 (administrative structures and materials), 5 U.S.C. 552 (FOIA) and 5 U.S.C. 552a (the Privacy Act). All requests for agency records are processed under FOIA, except to the extent they are first-party requests for records from a Privacy Act system that are fully granted under the Privacy Act alone. First-party requests for Privacy Act records that are not fully granted under the Privacy Act are processed under both the Privacy Act and FOIA. No agreements authorize information sharing. The DOJ guidance governs consultations and referrals with other agencies. The White House requires FOIA offices to consult with it on records implicating White House equities. Executive Order 12600 governs the submitter notice process.
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.	Name
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.	09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet 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 No. 0910-0832 Expiration Date: 6/30/2026
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 have the option to opt out of having their PII collected by choosing not to submit a record request. However, if they wish to submit a request but choose not to provide PII, the FDA cannot provide a response to their FOIA inquiry. When FOIA requests are submitted, some PII is needed in order to provide a response and to certify the requestor's identity. At the very least, this will be a name and email address. An individual requester can choose which contact information to provide to the FOIA office and which method to use to submit a request (e.g., do not need to use the online method, they may use mail, parcel delivery, or facsimile). A third-party requester can also make a request anonymously through a nominee with FDA using the nominee contact information to issue a response. The subject of PII contained in records gathered for FOIA requests may not opt out. By performing work for the government and using government systems and resources their work context PII is necessarily captured in agency records subject to record retention and disclosure requirements.

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.	No major changes are planned. However, if the FDA changes its practices with regard to the collection or handling of PII related to the CDRH FOIAXpress 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 email to individuals, adding or updating online notices or forms, or other available means to inform the individual. In addition, HHS/FDA would publish a revised System of Records Notice (SORN) in the Federal Register, update the PIA, and update any Privacy Act Statements as needed.
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 options available for assistance. These individuals may contact FDA offices, including the FDA FOIA office, the Privacy Office, the Employee Resource and Information Center (ERIC, a resource for FDA personnel), the Cybersecurity Infrastructure Operations Coordination Center (CIOCC, responsible for receiving reports of information incidents from FDA personnel) and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel and contractors must report that without delay to the 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.	Requester's PII is provided voluntarily by the individual. The individual is responsible for providing accurate contact information at the time of request. The information is copied from the AIMS system into FOIAXpress by CDRH FOIA personnel, who ensure its accuracy. The FOIAXpress system verifies the email address to ensure it is valid. PII relevancy is supported through the design of fields and forms to solicit only the PII that is necessary. 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 NIST's Federal Information Processing Standards (FIPS) 199. CDRH performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified in the course of system use are addressed when discovered
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: FOIA Office staff and FOIA Coordinators will have access to PII pertaining to requests they handle for purposes of handling the requests, submit requests and related communications to FOIA staff, and receive responses to same. Administrators: Administrator-level access will be granted only to certain users in the CDRH FOIA Office. Administrators will have access to PII for purposes of maintaining and updating the system, administering user access, and troubleshooting system problems. Contractors: Some of the system's users are Direct Contractors. They will have access to PII for purposes of maintaining and updating the system, administering user access, and troubleshooting system problems. Any Direct Contractor retained to assist the CDRH FOIA Office with processing requests and appeals would have access to PII for purposes of providing that assistance.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to FOIAXpress must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.
PIA 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.	The relevant supervisor will indicate on the user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria.
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 take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that training has been successfully completed.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Because the users are information disclosure specialists, they receive specialized training on a regular basis at FOIA/PA conferences and workshops hosted by the FDA, DOJ, and outside vendors providing advanced instructions and guidance regarding safeguarding personal privacy information and avoiding improper disclosures of PII in particular contexts and with respect to specific types of records.
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).	The applicable records schedule is General Records Schedule (GRS) 4.2, Information Access and Protection Records; it prescribes retention periods ranging from approximately 2 years to 6 years after the date a case is closed. The system will be updated when a case is closed, will calculate when case records are eligible for destruction, and will generate a report of eligible cases each year, for use in deleting eligible electronic records and shredding eligible paper files.

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 user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	7/30/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	7/30/2025
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.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	8/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/5/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/5/2025
SAOP Review Comments:	Approved on behalf of the SAOP	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/5/2025 10:20 AM	BLAND, CRYSTAL	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	8/4/2025	8/4/2025 Per FDA's email: The PIA is experiencing an Archer error with question General 03: "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 1/23/2023. 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.	8-4-2025 EMAIL_PIA in Queue (CDRH FOIAXpress).pdf CDRH FOIAXPress PIA_SOP Approved.pdf