PTA / PIA: FDA - eFax - QTR2 - 2026 - FDA5271864

Created Date: 6/30/2026 2:14 PM Last Updated: 7/16/2026 2:21 PM

General Information

PTA / PIA Name:	FDA - eFax - QTR2 - 2026 - FDA5271864	**PTA / PIA ID:**	4612004
Component Name:	FDA - OC Electronic Fax Communication	**ATO Boundary Name:**	OC GSS4 Enterprise Tools and Services
Overall Status:	Complete	**# of Days - Open:**	16
Submitter:		**Submit Date:**	7/10/2026
Next Assessment Date:	07/15/2029	**Expiration Date:**	7/15/2029
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	Ernest Jenkins
PTA 01A:	POC Title and Organization	System Owner (FDA-OC)
PTA 01B:	POC Email Address	Ernest.Jenkins@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-7245
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/Privacy Impact Assessment was last approved, FDA made the following changes: updated contact information.
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) Electronic Fax Communication (eFax) solution is an enterprise-wide electronic fax solution. The eFax solution allows FDA employees and Direct Contractors to send and receive faxes from their computer (e.g., government furnished laptops) or FDA network enabled mobile devices through the FDA email system or the software vendor web client console. Faxes can be sent from mobile devices by attaching an attachment to a fax number as an email. It works the same as emailing any regular attachment to an email. The fax system determines if it needs to be routed to the fax servers by the suffix of efax.fda.gov. Also, mobile users that have access to FDA internal websites will be able to access the eFax web console (e.g., via Uniform Resource Locator (URL), or web address to send and receive faxes. The eFax solution is a component of a larger system, the FDA's General Support System (GSS) 4 for Enterprise Tools and Services. Other components of GSS 4 are addressed in separate assessments. The eFax suite gives FDA the benefit of a custom fax implementation for each FDA center with both centralized and distributed management capabilities. FDA employees and Direct Contractors can safely and securely send and receive faxes from their FDA-approved devices.

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.	Every person who is a “user” of the FDA eFax system is a permanent FDA employee or Direct Contractor who sends and receives messages via an FDA eFax account for authorized work purposes. There are no people outside the FDA domain that have access to the FDA eFax system. External recipients and submitters have their own non-FDA eFax accounts. As part of FDA’s use of eFax, the agency necessarily collects the following personally identifiable information (PII) from users and external recipients and submitters: user credentials, points of contact data (e.g., first and last name, email address (business and personal), and assigned eFax number). In addition, the content of incoming fax images is controlled by the submitter and may contain all types of PII the sender opts to include, such as: Social Security number (SSN), truncated SSN, Driver’s License number, mother’s maiden name, phone number (business and personal), mailing address (business and personal), data universal numbering system (DUNS), medical records, medical records number, patient ID number, certificates, education records, military status, foreign activities, taxpayer ID, date of birth, photographic identifiers, biometric identifiers, vehicle identifiers, financial account information, legal documents, device identifiers, employment status, and passport number. Other PII included is chart number and provider license number. As part of the FDA deployment of eFax, through the use of Mailbox Server, fax images are encrypted at rest and stored in the system database. Only administrators and authorized users can decrypt the fax images. Users of the FDA eFax system are identity authenticated into the FDA network using FDA’s Active Directory (the subject of a separate PIA) which collects basic contact information (i.e., first name, last name, email address, phone number). Communications within the FDA use secure hypertext transfer protocol secure (https). Transmissions reaching the FDA’s voice over internet protocol (VoIP) system in route to the target fax number are handled as analog communications. Analog communications cannot be encrypted. As part of performing agency business, FDA organizations will use eFax to send and receive faxes from business partners in industries that the FDA regulates such as pharmaceutical, cosmetics, and food and device manufacturers. In addition to providing enforcement and pre-decisional information within FDA and disseminating information to external stakeholders, eFax is useful for employees and Direct Contractors. The system is not designed to be a data repository, but the images faxed are stored in a secure file share in the FDA domain (internal to the Agency) for 30 days eFax also collects and stores the following non-PII data about external recipients of messages sent by FDA users: recipient fax number and the recipient company name.

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.	Active Directory
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 eFax solution capabilities meet the following FDA business objectives: a) desktop-based electronic fax communications (send and receive) for individual assigned user accounts; b) send and receive faxes from anywhere via FDA-approved devices; c) replace desktop fax machines; d) Fax transmission delivery to a shared network folder for group/team review. FDA employs eFax as an enterprise-wide electronic fax solution. It allows FDA employees and Direct Contractors to send and receive faxes from their assigned computers or mobile devices through FDA email or the software vendor (eFax) web client console. In addition, eFax enables users to scan documents and send them to internal and/or external recipients in accordance with applicable information sharing laws, regulations, policies and procedures. Those scanned images are stored in the eFax database (all encrypted) and may contain PII depending on the content of the transmitted materials as controlled by the sender. Access to this data is only available to the system administrator (for generating reports) and the FDA or external owner (sender) of the communication stream. FDA user eFax numbers are assigned by Administrators at the individual user and office level. Each user is responsible for the use of their eFax number. FDA does not reuse, recycle, reissue or reassign eFax numbers. The FDA eFax user groups consist of Service, Administrator, and End-user accounts. The intended users are FDA employees and Direct Contractors. There are no external users of the system. External recipients and submitters have their own non-FDA accounts. FDA user access to the system employs a Single Sign-On (SSO) approach employing multi-factor authentication of each individual user; there are no system-specific authentication credentials (e.g., username, password) housed in the system. eFax collects the following PII data from and about users for every transmission: points of contact data (e.g., first and last name, email address and assigned eFax number; this is typically work context contact information). FDA's eFax also collects PII about external recipients and submitters for every transmission, consisting of recipient and submitter fax number and name (entity or individual). The system also collects non-PII and PII that is contained within eFax messages. Incoming and outgoing fax images may contain all types of PII. The content of incoming/outcoming faxes is subject to the individuals and entities that send the fax; FDA does not control the content of transmissions from external sources. It is necessary for the FDA to collect the specified PII in eFax to secure the data, control access, and conduct

		communications necessary for authorized FDA activities. Entities and individuals transmitting PII about third-party individuals are subject to applicable state, local, sector-specific federal, and other data handling and privacy authorities that may require notice, consent and other requirements directed at protecting the privacy of third-party individuals. FDA users do not use name or other PII to retrieve information from the system. FDA does not share the PII temporarily stored in eFax with other systems, organizations or entities.
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://efax.fda.gov http://fax.fda.gov https://efax-jobtracking-adc.fda.gov/jtrwebclient/default.asp https://efax-jobtracking-wodc.fda.gov/jtrwebclient/ http://fax-jobtracking.fda.gov/jtrwebclient/default.asp
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.	<a>https://efax.fda.gov The purpose of the website is to allow eFax users to log into the efax web client to see their faxes. It uses the credentials of the user logged in and shows that info. This is accessed via a web browser. <a>https://efax-jobtracking-adc.fda.gov/jtrwebclient/default.asp <a>https://efax-jobtracking-wodc.fda.gov/jtrwebclient/ These two URLs are used to produce reports for eFax activity. This is currently only used by a group of select individuals in CDER. This is accessed via web browser. <a>http://fax.fda.gov <a>http://fax-jobtracking.fda.gov/jtrwebclient/default.asp These two URLs are used only by the eFax administrator to test changes before implementing into production.
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 Truncated SSN Taxpayer ID Number (TIN) Driver's License Number Passport Number Financial Account Information (e.g., account numbers, credit card numbers) Device Identifiers Vehicle Identifiers (e.g., VIN, license plate number) DUNS Biographical Information Name Date of Birth User Credentials Mother Maiden Name Certificates (e.g., training certificates) Education Records Employment Status/History Foreign Activities Legal Documents Military 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 Medical Information Medical Records Medical Records Number Patient ID Number Other Other

PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Others - Chart No., TIN, DUNS, Provider License number Other - Note: PII collected from/about the FDA users and external recipients and submitters is name, email address and eFax number. Incoming fax message content and images are controlled by the sender and can contain all types of PII as needed for agency purposes, including those marked above.
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 Grantees Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499
PIA 25:	For what primary purpose is the PII used?	The fax number is required to send/receive the faxes and to verify if transmittal is successful. The email addresses within eFax can be used to forward specific faxes via email. For PII beyond contact information, the purpose of use will vary based on the specific FDA organization involved in the communication.
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.	The eFax system has no intended functional use for SSNs and is not designed as an SSN repository. SSNs may be inadvertently captured and temporarily stored in the system if an individual includes SSN information within fax content.
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.	The eFax system does not intentionally solicit or use SSNs for identification purposes, nor is it designed as an SSN repository. E.O. 9397, as amended by E.O. 13478, is cited as the governing authority in the event that SSNs are inadvertently captured and temporarily stored in the system via inbound fax content. FDA offices that receive such communications are responsible for ensuring they have the legal authority to use any SSN received and to use it only as permitted.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S.C. 301, 44 U.S.C. sections 2904 and 3102 for the authority to establish systems, collect information, and employ processes as needed to execute business and conduct actions to maintain and gather records to satisfy legal requirements imposed upon agencies. Individual FDA programs handle information transmitted to/from them via eFax in accordance with laws, regulations and policies applicable to their specific work.
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 Hard Copy Mail/Fax Phone Email Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	eFax does not have its own Office of Management and Budget (OMB) information collection approval number, as the system is intended for use by FDA internal users only and does not directly collect PII from the public.
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.	PII may also be obtained as part of the details in a fax transmission. External transmitters of PII control the content of their communications. They may also choose not to use eFax when other methods of communication are available. Upstream sources of PII gathered by external eFax transmitters such as the subjects of third-party PII included in a communication are beyond the scope of this PIA; they would be subject to the privacy policies of the entity communicating directly with FDA via use of eFax.
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.	FDA users are notified of any major changes to eFax via email, system content and/or user guides, notification from their administrative supervisors. As necessary, FDA policies would be updated and made available to external users on FDA.gov. This PIA would also be updated and provide additional notice.

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 are concerned about the collection, use, disclosure, or accuracy of their PII may raise concerns with their management, their FDA point of contact (in the case of external submitters and data subjects) and may also contact the FDA Privacy Office directly using email, phone, fax or mail contact information provided on FDA.gov and the agency's internal intranet Privacy Office webpages or via FDA's Employee Resources and Information Center (ERIC). All FDA permanent employees and Direct Contractors are required to rapidly report any potential unauthorized disclosure or access to PII. All reports must be submitted to the FDA's Cybersecurity Infrastructure Operations Coordination Center (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.	Users and external recipients and submitters voluntarily provide PII about themselves. When submitting PII about third parties, they must comply with applicable notice and consent laws (e.g., state law). Submitters and recipients are responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves. Their contact PII is relevant and necessary to be granted controlled access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). PII relevance is ensured by the design of the system to collect only PII that is necessary (e.g., for system access control and accuracy of communications). Integrity and availability are protected by privacy and security controls selected and implemented during assessing the system for an Authorization to Operate (ATO) approval. Controls are selected based on National Institute of Standards and Technology (NIST) guidance related to the system's security categorization level, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. For FDA users, the Office of the Commissioner (OC) Assessment Team performs quarterly 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 system are addressed when discovered.
PIA 38:	Identify who will have access to the PII in the system.	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.	Administrators: FDA Administrators work with the Active Directory system that syncs with eFax to control access for FDA users. Administrators assign roles/permissions for all users of eFax. Some of the Administrators are Direct Contractors. Contractors: Direct Contractors who have access to the servers and perform configuration and installation functions for eFax.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrators, Developers, and some Direct Contractors with elevated privileges, as approved by agency officials, have access to system PII. Approval procedures and outcomes are documented. All users can view the name, email, and phone number of a point of contact. eFax enforces role-based access control (RBAC) and least privilege principles. Only the relevant and intended FDA user receives and has access to eFax communication content, which may include PII. Fax images are stored in the eFax database where they are encrypted. Only Administrators and authorized users can decrypt.
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.	eFax enforces role-based access control (RBAC) and least privilege principles. Through technical and administrative controls, users only have the required level of access to fulfill their job responsibilities.
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.	The FDA makes it mandatory for all FDA personnel to complete information security and privacy training every year. A portion of this training is dedicated to the protection and use of PII. 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.	Additional training specific to eFax is not provided. User instructions are available from eFax.

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).	FDA maintains the records in under the following National Archives and Records Administration (NARA) citation General Records Schedule (GRS) 3.1 item 020, Information technology operations and maintenance records. Disposition of these records is temporary. Records are destroyed 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use. The disposition of incoming documentation which is received via fax must be managed by the responsible Program Office in accordance with the appropriate FDA Records Control Schedule. The records should be filed in the program office official recordkeeping system, and when records contain PII, the responsible program office securely maintains the records and ensures they are accessed only by authorized personnel.
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 role base access restriction, 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 uses of firewalls, access controls, encryption of files, certificates or logs, and regular testing of information technology systems. Physical controls include that all system servers are located at FDA 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:**	7/10/2026
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:**	7/14/2026
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.	**# of Days - SOP Review:**	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	7/14/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 7/14/2026 All comments have been addressed. This PIA is ready for SAOP review and approval. 7/8/2026 Please see comment and update accordingly: **PIA-27A:** Please include in your response "E.O. 9397," even is the system doesn't use SSN it is inadvertently collected and stored.	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/16/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	2

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/16/2026 2:21 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	7/6/2026	Per FDA: PIA and Email attached	FW_ PTA _ PIA 527164 is ready for APA Review.pdf OC Electronic Fax Communications_SOP approved.pdf
PIA 27A	BLAND, CRYSTAL	7/8/2026	Please include in your response "E.O. 9397," even is the system doesn't use SSN it is inadvertently collected and stored.	
PTA 01	BLAND, CRYSTAL	7/14/2026	7/14/2026 FDA's Resubmission: Attached PIA	OC eFAX SOP apprv'd resubmitted 7.14.26.pdf