PTA / PIA: FDA - CFS - QTR3 - 2026 - FDA5271954

Created Date: 7/9/2026 10:02 AM Last Updated: 7/16/2026 2:19 PM

General Information

PTA / PIA Name:	FDA - CFS - QTR3 - 2026 - FDA5271954	**PTA / PIA ID:**	4624554
Component Name:	FDA - OC Cloud File Sharing	**ATO Boundary Name:**	OC Cloud File Sharing
Overall Status:	Complete	**# of Days - Open:**	8
Submitter:		**Submit Date:**	7/13/2026
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?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	7/24/2023
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	William Johnson
PTA 01A:	POC Title and Organization	Information Technology (IT) Specialist ODT/OIMT/OTD/DIO/IB/SIT
PTA 01B:	POC Email Address	william.johnson@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-6613
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 OC Cloud File Sharing since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Food and Drug Administration (FDA) Office of the Commissioner (OC) Cloud File Sharing (CFS) system is a modern content management platform that transforms how organizations work and collaborate to achieve faster results. The purpose of the OC CFS project is to enable internal FDA users (FDA permanent employees and Direct Contractors) to securely collaborate and share files/folders with external partners such as other Federal agency employees, private businesses and members of the public (typically other government agencies, state agencies, and private sector employees). FDA users and partners can share files and collaborate effectively through a secure FedRAMP cloud infrastructure. The OC CFS Platform is provided to FDA users as a Software as a Service (SaaS) model. In this service delivery model, the vendor is responsible for all service delivery layers (e.g., infrastructure). FDA users and its partners connect to the OC CFS application through their Web Browse or Sync Client. FDA users and administrators do not have access to the underlying infrastructure of OC CFS. FDA OC CFS system administrators are responsible for managing the FDA's OC CFS instance. This functionality is provided through the OC CFS Admin Console accessible through the Web Browser and allows for the ability to manage users and groups, control content including sharing and collaboration permissions, generate detailed audit reports and further restrict access to sharing content or deleting files. Access to the system is accomplished via Single Sign-On (SSO) authentication methods. OC CFS will collect the username and password provided via SSO authentication for first time access to the system. Thereafter, users will be able to access the system using an SSO token validated using the ping federate service and will not require credentials provided via SSO authentication. External users' access credentials are administered by Box, Inc. which is a third-party cloud content management platform being used to administer FDA's OC CFS system. While OC CFS provides AI capability, AI tools are currently not in use. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks

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.	Given the number of FDA user organizations and their various program missions, it is impossible to predict or accurately describe all categories of personally identifiable information (PII) data elements that might be collected and processed by the various FDA offices that use the OC CFS system. The nature and sources of the information gathered depend upon the business needs of individual FDA center organizations. Two categories of PII that will not be collected by the system are Social Security Numbers (SSN) and credit card numbers. The OC CFS system has an embedded data loss prevention policy that quarantines and prevents the uploading of these data elements into the system. Categories of PII collected may include the following: (a) Name; (b) Date of Birth; (c) Mother's maiden name; (d) Passport; (e) Biometrics; (f) Driver license number; (g) Education records; (h) Employment status; (i) Financial account information (excludes credit card numbers); (j) Mailing address (personal and business); (k) Email address (personal and business); (l) Telephone number (personal and business); (m) Military status; (n) Photographic identifier(s); (o) Medical Records/number; (p) User Credentials; (q) Certificates; (r) Legal Documents; (s) Foreign Activities; (t) Device identification numbers; and (u) DUNS number. This list is not exhaustive and may include other PII not identified here. All FDA users are authenticated prior to system access through SSO multi-factor authentication to provide secure access to their CFS accounts. Username and password provided via SSO authentication are collected and used for time access requests. The Health and Human Services (HHS) Rules of Behavior (RoB) document and Standard Operating Procedure (SOP) governing OC CFS use are provided to all users to ensure they are aware of their responsibilities, including to avoid sharing, processing, or transmitting any sensitive PII data elements while using the CFS system. External users do not have access to OC CFS and cannot send information to FDA users through OC CFS. External user capabilities are limited to being able to log in and view materials within the limits of the access restrictions to which they are subject. External users cannot upload their own information into OC CFS. These users can only receive files and collaborate via e-mail. External users' access credentials are administered by Box, Inc. which is a third-party cloud content management platform being used to administer FDA's OC CFS system. External users will be authenticated by their CFS username and password. External users will establish a CFS account if they do not already have one in order to collaborate with FDA users. PII in the system is retained on a temporary basis per National Archives Records Administration (NARA) retention and disposal schedules.
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 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.	FDA's use of OC CFS enables content collaboration through a secure cloud-based portal. FDA licensed users and contractors use OC CFS to share files, links and collaborate in real-time with other FDA users and with authorized FDA partners (external to FDA) identified as collaborators. OC CFS provides FDA users with the capability to store, maintain, and manage various types of data according to their mission needs. The FDA user's responsibility for complying with the FDA privacy policies and guidance when using the OC CFS system is governed by the HHS ROB. Within FDA, the methods of communication and collaboration vary; users employ a variety of tools to store, manage, retrieve and share information. There is also no single source of data and it is not possible to specifically identify the data that will be collected in the OC CFS system since the subject matter of the collaboration activities differs from one activity to another. Although OC CFS maintains a variety of different types of data, the agency applies controls and standards that govern data use and mitigate risks. FDA users are prohibited from storing, processing, or transmitting any sensitive PII data elements within the OC CFS application. Before they are provided access to the OC CFS environment, FDA users are required to electronically sign the OC CFS ROB document which defines the requirements and limitations for data elements allowed within OC CFS. Internal FDA licensed users and Direct Contractors are automatically designated as OC CFS collaborators based on acceptance of the internal ROB. External FDA partners are required to electronically sign an external ROB agreement to operate as a collaborator and thus accept and/or collaborate on content and files developed by the FDA. This is collected outside the application. The OC CFS Administrator manages CFS built-in controls for identifying and quarantining SSNs and credit card information. Additional Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) tools are under development for future integration into the system.
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://fdahhs.account.box.com/login
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 purpose of the website is to allow users to accomplish work tasks anywhere, by sharing information, collaborating, and utilizing the storage capability within OC CFS. OC CFS also provides a means to coordinate work activities, the transfer of documents, and work collaboration. Users of the website include FDA permanent employees and Direct Contractors. Users access the website via the OC Cloud File Sharing uniform resource locator (URL).
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Driver's License Number Passport Number Financial Account Information (e.g., account numbers, credit card numbers) Device Identifiers 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 Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	The PII elements checked above are capable of being added to the OC CFS environment. However, this list is not exhaustive and may include additional categories of PII not captured here. The OC CFS system has an embedded data loss prevention functionality that automates the FDA's system-specific policy prohibiting the upload of SSNs and credit card information; the system quarantines attempted uploads containing SSNs and credit card numbers. This technical data minimization may be expanded in the future to limit the proliferation of additional PII.

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 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.	1,000,000 or more
PIA 25:	For what primary purpose is the PII used?	Name and email address are required to access OC CFS. Other PII found in materials handled within OC CFS is used for program-specific, mission-related collaboration.
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 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	General authority for implementing regulations for the usual and necessary infrastructure of running an organization is provided to agencies by 5 United States Code (U.S.C.) 301. Specific information use and disclosure authorities will differ for each agency organization using OC CFS based on the nature of the organization's work and the records used by its personnel.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet
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.	OC CFS does not collect information using an information collection request as defined by the Paperwork Reduction Act (PRA). The individual FDA user organizations and offices that use the OC CFS system are required to ensure that any associated information collections have been reviewed by FDA Paperwork Reduction Act officials and approved by the Office of Management and Budget (OMB) prior to collection.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes

PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Within HHS: Purposes for these disclosures are specific to the business needs of individual organizations and initiatives as well as applicable laws and policies governing the use of the disclosed PII. Other Federal Agency/Agencies: Purposes for these disclosures are specific to the business needs of individual organizations and initiatives as well as applicable laws and policies governing the use of the disclosed PII. State or Local Agency/Agencies: Purposes for these disclosures are specific to the business needs of individual organizations and initiatives as well as applicable laws and policies governing the use of the disclosed PII. Private Sector: Purposes for these disclosures are specific to the business needs of individual organizations and initiatives as well as applicable laws and policies governing the use of the disclosed PII.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Two ROB documents developed for external and internal users are signed by all users and govern data sharing and disclosure. The agreement governing information exchange with other agencies for OC CFS is defined within the external ROB requiring an electronic signature by any external entity looking to share data and collaborate with the FDA.
PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	Any submissions of PII are automatically quarantined. Data cannot be used by users without review and release by administrators. Logging is not required for tracking the sharing or disclosure of PII because that sort of behavior by default is not allowed. Any data with driver's license, credit card, or social security numbers is automatically quarantined by default and can only be cleared through administrator intervention. Administrators will only release files from quarantine if determined to be false positives. Data that truly contains PII upon review shall remain in quarantine.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals who wish to voluntarily access (use) the OC CFS system will be required to submit their name and work email address to establish access. This data is necessary for access control, and the system functions involve document collaboration and project related communications, networking between team members and knowledge sharing. For collaboration materials within OC CFS that contain PII about individuals who are not OC CFS users, the agency program that initially collected the PII is responsible for notice, consent, opt-out and other privacy 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.	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 formal process involving written and/or electronic notice at the time of hire, via internal broadcast email or informal processes such as email notice to the individuals.
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 a number of avenues available to resolve the situation. Employees may submit concerns to their supervisor, the FDA Privacy Office, the Employee Resource and Information Center (ERIC- a 24-hour technical assistance line), or FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). All FDA personnel are required to immediately report any suspected data breaches and security incidents to 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.	Currently, there is no process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Users and source system management are responsible for the accuracy of PII provided to OC CFS. Due to the array of PII and variety of data context and sources there is not a master source of data or other reconciliation vehicle enabling reviews of all the PII in OC CFS.
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: Authorized users may view content for work collaboration. Administrators: Individual administrators may have access to PII such as email address and name which is required to use the OC CFS system. They are not able to view non-explicitly authorized content and are subject to FDA rules and regulations on use and access. Contractors: Based on business requirements Direct Contractors can function as either Administrator or User. However, administrative privileged accounts are only used for administrative purposes. Functional use of the OC CFS system requires a separate user account.
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 OC CFS must have supervisor approval before access is granted. OC CFS administrators have full access throughout the entire OC CFS system. OC CFS users have access to their individual uploaded content, content explicitly shared through permission granted by the administrator, and content shared via collaboration or shared links. OC CFS external users have access to content explicitly shared via collaboration or shared links.
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.	No one is permitted access to the OC CFS portal unless specifically granted access by the OC CFS administrator. There are role-based access controls in place to minimize the amount of information to only that which is necessary for the role-based account, and per administrator assigned permissions and collaboration permissions. Supervisors indicate on the account creation form the minimum information system access that is required in order for the user to complete his/her job. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
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 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.	OC CFS Administrators will receive specialized training through the vendor's education portal. Users will be provided training through the Internal FDA OC CFS website which contains User Guides, Tri-folds, frequently asked questions (FAQs) and instructional videos. 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).	All FDA Center/Offices use National Archives and Records Administration (NARA) General Record Schedules to manage the disposition of administrative records and FDA Programmatic Record Control Schedules (RCS) to manage the disposition of Agency-wide records. The OC CFS system does not have Records Management capabilities to identify and implement the variety of records control/retention schedules applicable to the different types of records that may be stored in the system. Records that FDA programs chose to maintain within OC CFS are subject to the record control schedules of their specific FDA program office and record types. Schedule adherence is typically a manual process, and it is the responsibility of the user programs to maintain records in accordance with the applicable NARA schedule. Records in this system that contain PII are stored in secure file, and only authorized personnel have access. If program staff have questions regarding record schedules, they contact the appropriate FDA Center/Office Assistant Records Liaison Officer to ensure they are following appropriate record keeping practices. At a minimum, all data in Box is subject to the minimum data retention policy of 7 years. Any data, even if deleted by the user is still retained for a minimum of 7 years and is thus beyond the mandate of federal records retention schedules.
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 controls include user training and access approval procedures supporting need-to-know and least privilege access. Technical methods include role-based access settings, multi-factor authentication, firewalls, continuous monitoring and suspicious activity alerts and log aggregation and others. Physical controls include lock and key security of space and equipment and guarded facilities. Other appropriate controls have been selected from the National Institute of Standards and Technology (NIST) 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:**	7/13/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	7/13/2026
SOP Review Comments:	This is a resubmission 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. 7/9/2026 Note the Archer error associated with question General 03: "Does the system have or is it covered by a Security Authorization to Operate (ATO)?" The FDA instance of Archer is automatically entering the answer "No" which is incorrect. At this time, we are unable to update Archer to reflect the correct answer "Yes." The ATO date is 7/24/2023. The FDA Archer Team is aware of this occurrence and is working on a solution.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	7/13/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 7/13/2026 All comment(s) have been addressed. This PIA is ready for SAOP review and approval. 7/10/2026 Please see comment and update accordingly: **PIA-44:** FDA's response only **partially answers** the question it doesn't: 1) Cite specific NARA or FDA records schedules, 2) The retention periods are not tied to the schedules: The response states that Box retains data for at least seven years, but it does not explain whether that is a technical retention policy or the official records retention period under an approved NARA schedule. If different record types have different retention periods, that should be stated explicitly. 3) The destruction process is not described: FDA's response explains retention responsibility but does not explain how records are destroyed after the applicable retention period expires (e.g., in accordance with NARA-approved schedules, disposition by authorized personnel, secure deletion, etc.). • Which FDA Records Control Schedule (RCS) applies to records stored in OC CFS? • Are any NARA General Records Schedules (GRS) applicable (e.g., for administrative records), and if so, which ones? • Are we saying that the Records maintained in the OC CFS system are subject to the records schedule applicable to the owning FDA program office and the specific record type and that the Program Center/Office Assistant Records Liaison Officer will work with NARA to determine the applicable records schedule?	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/16/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/16/2026 2:19 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	7/9/2026	Per FDA: Email and PIA attached	PIA Submissions.pdf OC Cloud File Sharing SOP appvd 7.9.26.pdf
PIA 44	BLAND, CRYSTAL	7/10/2026	FDA's response only **partially answers** the question it doesn't: 1) Cite specific NARA or FDA records schedules, 2) The retention periods are not tied to the schedules: The response states that Box retains data for at least seven years, but it does not explain whether that is a technical retention policy or the official records retention period under an approved NARA schedule. If different record types have different retention periods, that should be stated explicitly. 3) The destruction process is not described: FDA's response explains retention responsibility but does not explain how records are destroyed after the applicable retention period expires (e.g., in accordance with NARA-approved schedules, disposition by authorized personnel, secure deletion, etc.). • Which FDA Records Control Schedule (RCS) applies to records stored in OC CFS? • Are any NARA General Records Schedules (GRS) applicable (e.g., for administrative records), and if so, which ones? • Are we saying that the Records maintained in the OC CFS system are subject to the records schedule applicable to the owning FDA program office and the specific record type and that the Program Center/Office Assistant Records Liaison Officer will work with NARA to determine the applicable records schedule?	
PIA 44	BLAND, CRYSTAL	7/13/2026	Per FDA's Email provided clarification for PIA-44 response: The response provided for PIA-44 was previously approved in the 2021	FDA - CFS - QTR3 - 2026 - FDA5271954_PIA44.pdf

PIA. We shared this information when meeting with our records management POC to inquire about current schedules. As was the case with the last iteration of the approved PIA, this response was confirmed to be acceptable given the nature of the cloud environment. Given the number of uses of the system throughout FDA it would be impossible to provide schedules for all use cases. Records maintained in the OC CFS system are subject to the records schedule applicable to the owning FDA program (or user program) office and the specific record type, and it is the responsibility of FDA office using the system to maintain records in accordance with applicable NARA schedules.
At a minimum, all data in Box is subject to the minimum data retention policy of 7 years. Any data, even if deleted by the user is still retained for a minimum of 7 years and is thus beyond the mandate of federal records retention schedules.