Privacy Impact Assessment (PIA): FDA - CFS - QTR2 - 2022 - FDA2041784

Date Signed: 4/14/2022

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1439931
PIA Name:	FDA - CFS - QTR2 - 2022 - FDA2041784	**Title:**	FDA - OC Cloud File Sharing
OpDIV:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Contractor
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
PTA - 5A:	If yes, Date of Authorization	8/7/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	There are no updates to the system that impact personally identifiable information (PII) since the last PIA.
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	External Cloud File Sharing is a modern content management platform that

		transforms how organizations work and collaborate to achieve faster results. The purpose of the FDA's External Cloud File Sharing (CFS) project is to enable internal FDA users (FDA 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).
PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	CFS is an external file sharing application that makes collaboration effective across devices, teams, and organizations. FDA users accomplish work tasks anywhere, by sharing information, collaborating, and utilizing the storage capability within CFS. CFS also provides a means to coordinate work activities, the transfer of documents, and work collaboration. Due to the variety of FDA user organizations and their various program missions, it is impossible to predict or accurately describe all the specific data elements that might be collected and processed by FDA offices that use the CFS system. The nature and sources of the information gathered depend upon the business needs of individual FDA center organizations. The CFS system has an embedded data loss prevention policy that quarantines and prevents Social Security numbers (SSNs) and credit card numbers from being uploaded into the system. A Rules of Behavior (RoB) document and Standard Operating Procedure (SOP) governing 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. All FDA users are authenticated prior to system access through single sign-on (SSO) multi-factor authentication to provide secure access to their CFS accounts. For further details regarding this response, please see the attached "FDA OC Cloud File Sharing (CFS) Box PIA 6-10-2021.docx_KMott approved 4.6.2022.docx"

PTA -9A:	Are user credentials used to access the system?	Yes
PTA - 9B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	FDA's use of CFS enables content collaboration through a secure cloud-based portal. FDA licensed users and contractors

use 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. CFS provides the FDA users 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 CFS system is governed by the 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 CFS system since the subject matter of the collaboration activities differs from one activity to another.

Although CFS maintains a variety of different types of data, the agency applies controls and standards to govern data use and mitigate risks. FDA users are prohibited from storing, processing, or transmitting any sensitive PII data elements within the CFS application. Before they are provided access to the CFS environment, FDA users are required to electronically sign a CFS RoB document which defines the requirements and limitations for data elements allowed within CFS.

Internal FDA licensed users and Direct Contractors are automatically designated as CFS collaborators based on acceptance of the internal RoB. External FDA partners are required to electronically sign an external RoB 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 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 - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name Driver's License Number Mother's Maiden Name E-Mail Address Phone numbers Medical records (PHI) Certificates Education Records Military Status Foreign Activities Date of Birth Photographic Identifiers Biometric Identifiers Vehicle Identifiers Mailing Address Medical Records Number Financial Account Info Legal Documents Devices Identifiers Employment Status Passport Number User Credentials Others - The system provides FDA users the capability to store, maintain, and share any of the types of PII that could potentially include sensitive PII. The PII elements checked above are capable of being added to the CFS environment. The 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 - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Public Citizens Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors) Other

PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Name and email address are required to access CFS. Other PII found in materials handled within CFS is used for program-specific, mission-related collaboration.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	5 U.S.C. 301. Specific information use and disclosure authorities will differ for each agency organization using CFS based on the nature of the organization's work and the records used by its personnel.
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities Other Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet Private Sector Other
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 10A:	Identify with whom the PII is shared or disclosed and for what purpose	Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies Within HHS
PIA - 10A	Explain why (and the purpose) PII is shared with each entity or individual.	Within HHS: Purposes for these disclosures

(Justification):		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 - 10B:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Two Rules of Behavior (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 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 - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	Users are notified of the collection of their PII during new user training and during the

		account creation process. PII will be used in accordance with the uses enumerated in the underlying privacy documentation for each program office and their data collection. Users (personnel) are notified at the time of hire of the agency's use of their information in relation to their government work and are advised at every login of the absence of any expectation of privacy when using the agency network. Additional notice about CFS is provided to the public through this PIA.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	Individuals who wish to voluntarily access (use) the CFS system will be required to submit their name and work email address to establish access. This data is necessary for access control and because the system functions involve document collaboration and project related communications, networking between team members and knowledge sharing. For collaboration materials within CFS that contain PII about individuals who are not CFS users, the agency program that initially collected the PII is responsible for notice, consent, opt-out and other privacy requirements
PIA - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained	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 - 15:	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	Employees may seek assistance by email or telephone to a CFS customer service specialist if they have questions or concerns

		regarding information within the system. In some instances, (e.g., account creation) data in the system is supplied by FDA's internal Enterprise Administrative Support Environment (EASE) system and personnel may access their EASE data on their own to update or correct their information. External or Employee personnel may also contact FDA's Employee Resources and Information Center (ERIC) to correct inaccurate or out of date information and contact the CFS Administrator for assistance.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. 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 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 CFS.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17	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 CFS application. 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 CFS system requires a separate user account.
PIA - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	CFS administrators have full access throughout the entire CFS system. 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. CFS external users have access to content explicitly shared via collaboration or shared links.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	No one is permitted access to the CFS portal unless specifically granted access by the 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 - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	All agency personnel are required to complete IT security awareness training annually. This training includes guidance on identifying and protecting PII. Completion of awareness training is tracked by the Office of Digital Transformation (ODT). CFS Administrators will receive specialized training through the vendor's education portal. Users will be provided training through the Internal FDA CFS website which contains User Guides, Tri-folds, frequently asked questions (FAQs) and instructional videos.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	All end-user training will be accessible from the CFS Website through the use of User Guides, trifolds, FAQs and instructional videos.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific 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 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 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.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	The information contained within CFS is protected by technical, administrative, and physical controls. CFS is responsible for ensuring some basic administrative, technical, and physical safeguards for PII stored in the CFS Service as CFS manages the infrastructure, systems, and applications that makeup the CFS Service. Administrative controls include user training and access approval procedures supporting need-to-know and least privilege access. Technical methods include multi-factor authentication, firewalls, continuous monitoring and suspicious activity alerts, log aggregation and others. Physical controls include lock and key security of space and equipment and guarded facilities.