Privacy Impact Assessment (PIA): FDA - eDiscovery - QTR3 - 2022 - FDA2063850

Date Signed: 2/6/2023

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:**	1489245
PIA Name:	FDA - eDiscovery - QTR3 - 2022 - FDA2063850	**Title:**	CTP eDiscovery
OpDiv:	FDA		

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	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.	CTP eDiscovery for Document Review (eDDR) is an eDiscovery platform that provides for the

		organization of large amounts of data in a single solution used by FDA's Center of Tobacco Products (CTP) within the Office of Compliance and Enforcement (OCE). It facilitates finding and preparing evidence and allows for the examination and secured sharing of digitalized evidence used for ongoing investigations. Evidence and information is gathered, analyzed and maintained in preparation for use in litigation. As used by CTP, eDDR provides a document repository for digital evidence, scanned versions of documents, and other evidence relevant to specific investigations. It may contain digitalized evidence that has been recovered via FDA investigators, private sector sources, anonymous sources, social media sources, and pertinent information recovered or obtained from other sources during an investigation. Sources of collected evidence and information also include physical hard copies and electronic copies of documents recovered from regulated entities. Regulated entities can consist of individuals, groups, businesses, and other organizations as well as any other place or source specified in a court order or other legal authority. Evidence may also be collected directly from prospective witnesses and/or people under investigation.
PTA - 5:	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.	The documents and materials CTP maintains in eDDR may contain PII and other information including but not limited to: financial account

		information, work and personal email communications, receipts, laboratory reports, medical record information, medical notes, Social Security number, driver's license number, name, mother's maiden name, phone numbers, certificates, date of birth, photographic identifiers, vehicle identifiers, personal mailing address, legal documents, device identifiers, and passwords. The documents recovered may also include office location and other administrative or work contact information. The information in CTP eDDR also includes non-PII such as information about FDA-regulated products related to an agency investigation of misbranding, tampering, counterfeiting, buying, and/or selling such products illegally. This information is necessary for OCE enforcement activities.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 6:	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.	OCE uses eDDR to store digital data on secure physical and virtual servers located within FDA

Headquarters. OCE's instance of eDiscovery uses multi-factor authentication with a Personal Identity Verification (PIV) card to control access. eDiscovery is only accessible by approved OCE staff (permanent FDA employees) with elevated privileges and/or access that is granted to users by an eDiscovery Administrator. Users are provided access by account creation by the eDiscovery Administrator. Permissions are granted where least privileges are enforced, and user access is granted on a case-by-case basis.

Evidence collected from the various sources includes information about individuals such as the subjects of investigations. Subjects of an investigation are typically members of the public, and in some instances may be permanent or contract employees of the FDA. OCE may investigate any persons where there is indication or signs of improper activity as it relates to misbranding, counterfeiting, tampering, buying or selling products illegally. The system also contains information about FDA personnel who are not the subject of an investigation.

Documents maintained in eDDR include information required by law enforcement for law enforcement activities. These documents may contain a variety of information ranging from financial to medical record information, as well as personal and administrative data and information about regulated products. Given the purpose of the system and the inherently variable information collected in investigative matters, it is not possible to exhaustively identify the data elements contained in the materials stored in the system.

Investigators using CTP eDDR retrieve system records in different ways including utilizing several PII elements to retrieve information about and/or gathered from subjects, witnesses and others involved in criminal activity during an investigation.

OCE uses eDiscovery to store digital data on secure physical and virtual servers located within OCE.

PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	No
PTA - 14:	Does the system have a mobile application?	No
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Mother Maiden Name Certificates Taxpayer ID Vehicle Identifiers Legal Documents User Credentials Driver License Number Email Address Education Records Date of Birth Mailing Address Devices Identifiers Patient ID Number Name Phone numbers Military Status Photographic Identifiers Medical Records Number Employment Status Medical records (PHI) Foreign Activities Biometric Identifiers Financial Account Info Passport Number Other - Free text Field - Information in eDiscovery files can be of any type. All documents are collected pursuant to an FDA investigation and are collected with the expectation that the information they contain may be relevant to those matters.
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 Grantees Patients

		Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
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?	PII in CTP eDDR is used to identify and associate individuals with actions and evidence in support of investigations of regulatory activity related to suspected violation of the U.S. Federal Food, Drug, and Cosmetic Act (21 U.S.C. 372) and other crimes.
PIA - 5:	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 - 6:	Describe the function of the SSN and/or Taxpayer ID.	SSNs maintained in CTP eDDR are not solicited or collected directly from individuals. SSNs may be maintained in the system incidentally when contained in documents collected during an investigation. CTP eDiscovery does not make use of the SSNs found in documents or other materials collected during investigations.
PIA - 6A:	Cite the legal authority to use the SSN.	N/A
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The legal authorities that govern information use and disclosures specific to the system and program are: Section 702 of the U.S. Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301, 372) authorizes OCE to conduct investigations. Secrecy and confidentiality of information is further governed by the Federal Rules of Civil Procedure (FRCP) Title III, Rule 6(e). 5 U.S.C. 301 authorizes the necessary establishment of systems and processes to maintain records and conduct agency activities. Further authority is provided by the Public Health Service Act (42 U.S.C. 201 et seq.) and Title 18, U.S.C. (e.g., 18 U.S.C. 201, 203, 207, 208, 209, 1905).

PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Investigators using CTP eDDR retrieve system records utilizing several different PII elements depending on the specific subject and nature of the investigation. Investigators may potentially use any type of PII collected or maintained in the system.
PIA - 8B:	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.	09-10-0002, Regulated Industry Employee Enforcement Records, HHS/FDA. Note that FDA will make appropriate updates SORN 09-10-0002 to reflect current technologies, organizational structures and office information and address eDiscovery records. 09-10-0013, Employee Conduct Investigative Records, HHS/FDA.
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Phone Email Online Other Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign Other Federal Entities Other Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet Private Sector Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10C:	Explain why an OMB information collection approval number is not required.	CTP eDiscovery is a tool used internally by the center so there aren't any Paperwork Reduction Act (PRA) implications.

PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Within HHS: The sharing of PII is dependent upon the nature of the investigation and whether it is a joint investigation being conducted with other federal or state law enforcement agencies including components of HHS. The PII in eDiscovery is not currently shared with other internal or external systems and no such sharing is expected. Other Federal Agency/Agencies: The sharing of PII is dependent upon the nature of the criminal investigation and whether it is a joint investigation being conducted with other federal or state law enforcement agencies. The PII may also be shared on an as-needed basis with criminal prosecutors (e.g., Department of Justice) who are involved in the investigation. The PII in eDiscovery is not currently shared with other internal or external systems and no such sharing is expected.
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	OCE may share investigative information with other federal agencies as part of joint investigations and pursuant to agreements under disclosure-controlling regulation, e.g., 21 CFR 20.85 (Disclosure to other Federal government departments and agencies). Information may also be shared with state or local authorities pursuant to agreements established under 21 CFR 20.88 (Communications with State and local officials). These regulations require the parties to execute specific agreements concerning the permissible uses of the shared information and to implement specific privacy and security controls. External law enforcement entities may also request Privacy Act records using processes provided under the statute and HHS and FDA regulations.
PIA - 11D:	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.	Disclosures to other federal, state, or local agencies are documented through written

		requests under 20 CFR 20.85 and 20 CFR 20.88 and through written responses to those requests. This practice also satisfies the accounting of disclosure requirements under the Privacy Act, 5 U.S.C. § 552a(c).
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Mandatory
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	Pursuant to Subpoena rules, Fed. R. Civ. P. 45 and Fed. R. Crim. P. 17, as well as applicable State law, PII maintained in eDiscovery is obtained through legal law enforcement authority via warrants and subpoenas. An individual who refuses to provide his/her PII in response to a subpoena may be subject to civil or criminal penalties.
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	Subjects under investigation are not able to opt out of the collection of their PII. That may completely jeopardize an investigation. They are unable to opt out because PII is obtained through legal law enforcement authority via warrants and subpoenas. As is the nature of investigations, in many instances PII is collected from sources other than the subject individual. An individual who refuses to provide his/her PII in response to a subpoena may be subject to civil or criminal penalties. Under the Privacy Act and the applicable SORN(s), this system is exempt from certain requirements of the Privacy Act including notice of information collection and access to investigative records.
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.	No such changes are anticipated. Note that there is no notification and consent process regarding major changes affecting the investigative aspects of the system because information is obtained and used for federal investigative purposes and notification could compromise ongoing investigations. Relevant SORNs and HHS and FDA regulations specify that the investigative records in this system are exempt from the individual notice and other requirements of the Privacy Act (See 5 U.S.C. 552a(e)(3)).
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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have many avenues available for assistance. These individuals may contact

		FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the FDA Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone, and standard mail avenues (all listed on fda.gov and the FDA intranet). All FDA personnel are required to rapidly report any suspected and/or known breach to the SMC.
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.	Individuals must provide PII pursuant to subpoenas in civil and criminal court cases. The individual is responsible for providing accurate information. Accuracy is ensured, under penalty of law, by individual review at the time of reporting. FDA personnel voluntarily providing information, may correct/update their information themselves. Mandatory PII is relevant per legal requirements pursuant to investigations. Relevance of voluntarily provided PII is supported by the design of the system to require and collect only the PII elements necessary to administer the system and enable its intended use. 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 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. CTP performs annual reviews to evaluate user access.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	**Users**: Investigating Agents (users) require

		access to the data, which may contain PII, to review the various evidence collected concerning subjects. **Administrators:** Administrators will have access to PII data in eDiscovery: Administrators may be exposed to PII information during the process of providing restrictive access to data to the Investigating Agents. Enter the reason here **Contractors**: Assisting Investigating Agents, require access to the data, which may contain PII, to review the various evidence collected concerning subjects who are suspected of being involved in criminal activity.
PIA - 19:	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 the system 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 - 20:	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.	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 - 21:	Identify the general security and privacy awareness training provided to system users (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 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 individuals successfully complete the training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and	Retention time of the PII is dependent on the length of time a case remains open and

	include the retention period(s).	adjudicated. This practice is consistent with FDA Records Schedule 8900, Reference Materials, National Archives and Records Administration (NARA) Citation N1-088-05-1, which indicates that materials are destroyed or deleted when no longer needed for reference purposes.
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.	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.