Privacy Impact Assessment (PIA): FDA - CBER Connect - QTR1 - 2022 - FDA2033406

Date Signed: 1/31/2022

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:**	1416330
PIA Name:	FDA - CBER Connect - QTR1 - 2022 - FDA2033406	**Title:**	FDA - CBER Office of Regulatory Operations
OpDIV:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Implementation
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?	Agency
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)?	No
PTA - 5B:	If no, Planned Date of ATO	1/14/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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?	The purpose of the Center for Biologics Evaluation and Research (CBER) Connect system is to provide CBER's Regulatory Project Managers (RPM) the

		ability to electronically search, view and upload industry submissions, communications and CBER Programmatic Items as part of the industry submission review process. CBER Connect v1.0 was the initial release of CBER's modernized User Interface (UI) for accessing regulatory review functions. It provides document access, search, and upload capabilities. Key features include screens for accessing industry submissions and FDA generated communications. CBER Connect provides the ability to conduct full-text searches by keyword for FDA generated communications and public Programmatic Items in the CBER Search Home Screen. CBER Connect also introduces a modernized UI for users when interacting with another system, CBER's Electronic Records (CER).
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.	CBER Connect is the primary point of entry for CBER staff to conduct regulatory and non-regulatory business, resulting in fewer UIs for users to navigate. As part of the CBER

modernization initiative, CBER Connect provides regulatory reviewers access to submission data for submission processing. CBER Connect users (FDA employees and Direct Contractors) access the system via a Single-Sign-On (SSO) process using multi-factor authentication.

To facilitate the submission review activity, CBER Connect processes personally identifiable information (PII) that includes: (a) name; (b) email address; (c) phone numbers; (d) medical notes; (e) date of birth; (f) certificates; (g) clinical study data; and patient identifiers such as (h) photographic identifiers; (i) biometric identifiers; and (j) and medical records numbers. The PII data is not directly collected from patients and are not shared with any other system or organization. Additional information about the IT systems and product application artifacts processed using CBER Connect during the submission review include:

Premarket Approvals (PMAs): FDA approvals to manufacture or distribute certain medical devices. PMAs include new drug applications for a device under section 520(l) of the FD&C Act.

Premarket Notifications 510(k): FDA premarket approvals for devices, not subject to a PMA themselves, to demonstrate that the devices to be marketed are at least as safe and effective (that is, substantially equivalent) to an already-legally marketed device.

Investigational Device Exemptions (IDEs): FDA approvals for producers to use investigational devices in clinical studies, in order to collect safety and effectiveness data.

Investigational New Drug applications (INDs): FDA approvals for producers to use new biological compounds, vaccines, blood and blood components, as well as human and non-human tissues and factors in clinical studies, in order to collect safety and effectiveness data.

Biologic License Application (BLA): FDA approvals to manufacture or distribute certain new biological compounds, vaccines, blood and blood components, as well as human and non-human tissues and factors. BLA includes a new biologic application for the entities covered in 21 CFR 600 series.

Master Files (MF): FDA approvals to manufacture certain new biological compounds, vaccines, blood and blood components, as well as human and non-human tissues and factors. These documents are not reviewed until they are cross-referenced in a BLA or IND application.

New Drug Applications (NDAs) and abbreviated New Drug Applications (ANDAs): FDA approvals to manufacture or distribute certain new biological compounds.

PTA -9A:	Are user credentials used to access the system?	No
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	CBER Connect is the primary point of entry for CBER staff to conduct regulatory and non-regulatory business, resulting in fewer UIs for users to navigate. As part of the CBER

modernization initiative, CBER Connect provides regulatory reviewers access to submission data for submission processing. CBER Connect users (FDA employees and Direct Contractors) access the system via a Single-Sign-On (SSO) process using multi-factor authentication.

To facilitate the submission review activity, CBER Connect processes personally identifiable information (PII) that includes: (a) name; (b) email address; (c) phone numbers; (d) medical notes; (e) date of birth; (f) certificates; (g) clinical study data; and patient identifiers such as (h) photographic identifiers; (i) biometric identifiers; and (j) and medical records numbers. The PII data is not directly collected from patients and are not shared with any other system or organization. Additional information about the IT systems and product application artifacts processed using CBER Connect during the submission review include:

Premarket Approvals (PMAs): FDA approvals to manufacture or distribute certain medical devices. PMAs include new drug applications for a device under section 520(l) of the FD&C Act.

Premarket Notifications 510(k): FDA premarket approvals for devices, not subject to a PMA themselves, to demonstrate that the devices to be marketed are at least as safe and effective (that is, substantially equivalent) to an already-legally marketed device.

Investigational Device Exemptions (IDEs): FDA approvals for producers to use investigational devices in clinical studies, in order to collect safety and effectiveness data.

Investigational New Drug applications (INDs): FDA approvals for producers to use new biological compounds, vaccines, blood and blood components, as well as human and non- human tissues and factors in clinical studies, in order to collect safety and effectiveness data.

Biologic License Application (BLA): FDA approvals to manufacture or distribute certain new biological compounds, vaccines, blood and blood components, as well as human and non-human tissues and factors. BLA includes a new biologic application for the entities covered in 21 CFR 600 series.

Master Files (MF): FDA approvals to manufacture certain new biological compounds, vaccines, blood and blood components, as well as human and non-human tissues and factors. These documents are not reviewed until they are cross-referenced in a BLA or IND application.

New Drug Applications (NDAs) and abbreviated New Drug Applications (ANDAs): FDA approvals to manufacture or distribute certain new biological compounds.

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 E-Mail Address Phone numbers Medical records (PHI) Certificates Date of Birth Photographic Identifiers Medical Records Number Others - Clinical study data that may contain identifiers.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Patients 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?	PII is used to contact regulated industry establishments regarding their applications while they are under review, during reviews of adverse event reports, when conducting trend analysis, and for analyzing outliers in clinical study data.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	Collecting this information is necessary to meet the FDA's requirements for conducting market submission review and post market surveillance under the provisions of the Federal Food, Drug, and Cosmetic Act at 21 U.S.C. 301, see especially sections 505A, 506B, and 522. Additional information concerning these activities may be found in CBER's regulations at 21 CFR 600.80.
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 Non-Government Sources Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	OMB Approval number 0910-0014 with expiration date 03/31/2022.

		OMB Approval number 0910-0001 with expiration date 03/31/2024.
PIA - 9B:	Identify the OMB information collection expiration date.	3/31/2022
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
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	There are no formal notice and consent procedures specific to this system. Submitters provide their contact information as a practical requirement in order to communicate with FDA about submissions. FDA personnel (employees) and Direct Contractors (vendors/suppliers/contractors) are notified at the time of hire of the agency's collection, creation, and use of their PII in context of their work with FDA. At network logon, personnel view and acknowledge a warning (text box) advising them of the lack of privacy when using government systems and resources. Product sponsors (submitters) that collect patient data are responsible for providing notice and obtaining consent from patients/clinical trial subjects. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet pages. This PIA provides further notice.
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 can opt out of the clinical trials that record the relevant patient data referred to as PII. This option and the process for doing so are provided to these individuals via consent forms provided by the trial sponsor. This occurs prior to submitting this information to FDA, and FDA does not have oversight of this part of the consent process. Industry points of contact provide PII as a mere convenience. No individual is required to provide this information, although FDA requests this information to facilitate communications with regulated industries. FDA personnel whose PII is in the system would be unable to perform their duties if they opted not to provide their PII.
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 FDA changes its practices with regard to the collection or handling of PII related to the website, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.

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 may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Systems Management Center (SMC) and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel must report immediately to the FDA's Systems Management Center (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	FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. PII relevancy is supported through 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 in the course of 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.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17 Users have access to PII in the course of reviewing applications for regulatory and scientific merit. Administrators ensure the proper controls are in place for user access, but administrators do not review industry-submitted content or FDA analysis of that content. Developers build new capabilities for reviewers to use, but they do not review industry-submitted content or FDA analysis of that content. Direct Contractors are sometimes developers and have access only to such material as developers have.	
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	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 - 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	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 - 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 system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that training has been successfully completed.
PIA - 21:	Describe 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 NARA records retention schedule(s) and include the retention period(s)	Records Control schedules are maintained for all data that traverses CBER Connect during the submission review process. Updating and maintaining those records schedules is the responsibility of CBER's Document Control Center (DCC) staff. The records schedules for the data processed in CBER Connect as follows: Investigational Files: FDA Schedule item B-10 N1-088-03-05 Biologic License Applications Files: The records are destroyed 30 years after being withdrawn or terminated. FDA Schedule item B-31 N1-088-03-05: The records are destroyed or revoked after 10 years. Master Files (FDA Schedule item B- 20 N1-088-03-05): The destruction of records in the system is done by withdrawing or terminating the records after 30 years. New Drug Applications (FDA Schedule item B-21 N1-088-03-05): The records are destroyed, revoked, or withdrawn after 10 years. Pre-Market Devices (510K) (FDA Schedule item B-22 N1-088-03-05: The records are destroyed, revoked, or withdrawn after 20 years. Pre-Market Application (PMA) (FDA Schedule item B-23 N1-088-03-05): The records are destroyed, revoked, or withdrawn after 30 years. Pre-Application Submissions: This is an unscheduled item with the Records Control Schedule under development.
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.