Privacy Impact Assessment (PIA): FDA - STARSWEB - QTR2 - 2021 - FDA1951005

Date Signed: 10/18/2021

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:**	1325199
PIA Name:	FDA - STARSWEB - QTR2 - 2021 - FDA1951005	**Title:**	FDA - CVM Corporate Database Portal
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?	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)?	Yes
PTA - 5A:	If yes, Date of Authorization	8/30/2019
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	There have been no privacy related changes to the system since the last Privacy Impact Assessment (PIA) was completed.
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 Corporate Database Portal system (CDP) is a web-based application consisting of several integrated modules sharing a common database

		used by FDA Center for Veterinary Medicine (CVM) employees to track and report on their work. CDP uses web services to share data and integrate with other FDA/CVM systems. The system supports activities related to pre-market approval of animal drugs and animal food additives, post-market animal drug safety surveillance activities, compliance activities, export certificate activities, animal drug listings and establishment registrations, bioresearch monitoring of animal drug studies, time reporting tracking, and minor use/minor species drug index files.
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.	CDP contains information on: pre-market animal drugs and feeds such as research sponsor name (corporate owner), active drug ingredients, indications for use, and relevant species; post-market safety of animal drugs and feeds (such as adverse drug events and drug experience reports); animal drug products and related establishments (i.e., manufacturers and distributors); employees' daily activities and times worked; animal drug research monitoring (clinical investigators, contract research labs, manufacturing sites); correspondence contacts; export certificates; regulatory actions; and similar FDA programs administered by CVM. The system collects this information to track the drug approval process and other administrative functions performed by CVM in accordance with the Federal Food, Drug, and Cosmetic Act (FD&C Act). The personally identifiable information (PII) in this system consists of name and professional contact information, such as office address and phone number of clinical investigators and research sponsor personnel serving as the sponsoring entity's point of contact for interaction with FDA and animal owners. Additionally, the system collects and maintains name and office phone number of CVM personnel who use CDP. PII about CVM personnel using CDP is collected for activity time reporting and other administrative purposes. Submission of this information is required in order to comply with the FD&C Act. The only individuals who can access the CDP system are CVM employees including direct contractors who have been approved as CDP users. Once approved, CDP users access the system via a single-sign-on (SSO) process using multi-factor authentication. CDP does not require, use, collect or maintain system-specific user logon credentials (e.g., username and password).
PTA -9A:	Are user credentials used to access the system?	Yes
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	CDP is the CVM's main transactional database that supports various data applications for CVM divisions such as CVM's Office of New Animal Drug Evaluation (ONADE), Office of Surveillance

		and Compliance (OSC), Office of Research (OR), Office of Minor Use, Minor Species (OMUMS), and Office of Management (OM). It is comprised of three application systems: CDP, CDP-Web, and the Compliance Log system (LOG). It is a relational database system consisting of several subsystems. CDP supports common data tables with, and provides a link to, CVM's Corporate Document Management System (CDMS). CDP is the entry portal for six modules for data entry, data storage, data tracking and reporting throughout CVM: Submission Tracking and Reporting System (STARS), Drug Experience Reporting System (DERS), Drug Product Listing (DPL), Bioresearch Information Monitoring (BIMO), Minor Use/Minor Species (MUMS) Index File System (MIFS), and Activity Time reporting (ATR). These CDP modules support pre-market and post-market business processes related to safety, product quality, administrative, food safety, drug indexing, bioresearch monitoring, and compliance. They enable FDA to administer and manage the review and processing of data necessary to ensure the quality and safety of animal drugs. This includes processing animal drug application submissions, maintaining post-market animal drug and feed safety reporting information, and performing internal accounting tasks. CDP-Web is the Java-based version of the user interface, currently providing access exclusively to STARS. The Compliance Log System (LOG) used by the Division of Compliance consists of three modules: (1) The Correspondence Tracking module that tracks correspondence received by the division with regard to animal drugs and provides various internal reports; (2) The Regulatory Action module that tracks regulatory actions taken against a company or person subject to animal drug regulations(various types of reports are available for management use); and (3) The Export Certificate Logging module that tracks information related to requests for animal drug and animal food/feed export certificates. Information from this module is sent to the Office of Financial Management (OFM) to invoice those external customers requesting certificates for billing purposes.
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

		Mailing Address Others - All contact information is assumed to be professional contact information, it may also be personal capacity PII for individuals doing business under their own names.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Public Citizens Other - "Public Citizen" above refers to animal owners, laboratory personnel (contact persons), clinical investigators, drug manufacturer (contact persons), or veterinarians.
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 about FDA is used for time reporting. PII about members of the public is used as professional contact information, namely regulatory contacts for external stakeholders doing business with FDA.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	Information in this system is collected, used and disclosed pursuant to the Federal Food, Drug and Cosmetic Act (FFDCA), 21 U.S.C. 301. Provisions of the FFDCA require regulated entities to maintain records and submit reports to FDA and CVM, e.g., sections 360b (1), 360cc and 379.
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Online Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	0910-0284, 03/31/2021 (FDA 2301) 0910-0032, 07/31/2022 (FDA 356v) 0910-0645, 06/30/2022 (FDA 1932 & 1932a) 0910-0454, November 30, 2022 (FDA 3538) 0910-0498, April 30, 2021 (FDA 3613, 3613a & 3613b).
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	Within HHS
PIA - 10A (Justification):	Explain why (and the purpose) PII is shared with each entity or individual.	Within HHS: FDA's Office of Financial Management (OFM). Sharing is restricted to need-to-know for the performance of authorized agency activities.

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)).	None. Disclosures are within FDA and restricted to need-to-know for the performance authorized agency activities.
PIA - 10C:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII	FDA does not expect or plan to disclose records in this system to any individuals or entities outside of FDA. This is not a Privacy Act system of records, and the Act does not require that FDA/CVM maintain an accounting of disclosures.
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	CVM personnel are also notified at the time of hire of the Agency's collection, creation, and use of their PII in context of their work with the Agency. External submitters receive notice on a submission form. In the online form, instructions and guidance, and the privacy policy are available via a hyperlink. 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	In many cases, submission of information to this system is required in order to conduct business related to animal feed and drugs in the United States. Clinical investigators, veterinarians, animal owners and other external submitters receive notice as displayed on the submission forms; on fda.gov where the various submission processes are described and where a link to the FDA privacy policy is permanently displayed; and within the relevant statute, regulations and related Federal Register notices. In addition, certain submission forms provide for submitter confidentiality or allow the submitter to choose whether his/her identity is disclosed to the manufacturer of a drug about which an adverse event or problem report is submitted. For employees, there is not a notice/consent or opt-out process specific to the CDP system. At the time of hire, CVM personnel are given notice of and consent to FDA's use of their professional information in relation to their work as a federal/FDA employee. They can update and correct the information at any time through existing procedures.
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 CDP system, the Agency will employ 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 have several options available to resolve the situation. These individuals may

		contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes. Employees with such concerns can additionally work with their supervisors, the Privacy Office, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels. Contact information for these offices and resources is available across FDA's internet and intranet pages.
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	An individual's PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. Incorrect data is corrected in the course of FDA/CVM's use of the system/information, e.g., updating name and phone number for entity point of contact. Accuracy is ensured by individual review at the time of submission. FDA personnel may correct/update their information themselves. Individuals external to the FDA, may contact the FDA through phone or email to correct their PII. PII relevancy is ensured by the design of forms, web pages and other data collection methods to allow only for the submission of PII that is essential for necessary and authorized uses. Access to PII 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 National Institute of Standards and Technology (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. CVM performs annual reviews to evaluate user access
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: Receive, review, manage and track submissions. Some of the users are Direct Contractors. Administrators: Monitor the system, manage the workflow and system access. Contractors: "Contractors" refers to FDA Direct Contractors who receive, review, manage and track submissions.	
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	Users who require access to the information system must obtain written supervisor approval and sign off before access is granted. The user's

		supervisor will indicate on the account creation form the minimum information system access that is required in order for the user to complete his/her job.
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	All users of the system may require access to any and all PII in the system. While access requires authorization, all users need and have access to all PII. The access list for the information system is reviewed on a semi-annual basis during which time 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 system users at FDA complete 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 - 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)	There is currently no records schedule in place. A job request seeking an approved retention schedule is in development for submission to the National Archives for approval. Once the Agency has received notice from the National Archives, CVM will update the PIA with the appropriate records schedule.
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 NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.