Privacy Impact Assessment (PIA): FDA - FURLS - QTR1 - 2022 - FDA2034601

Date Signed: 6/28/2022

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:**	1429198
PIA Name:	FDA - FURLS - QTR1 - 2022 - FDA2034601	**Title:**	FDA - OC FDA Unified Registration and Listing System
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?	Yes

URL Details

Type of URL	List Of URL
Internet (publicly available)	https://www.access.fda.gov/

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	8/7/2019
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	The following modules have been added under the FDA Unified Registration and Listing System (FURLS): Center for Veterinary Medicine (CVM) Export Certification Application and Tracking System (CVM eCATS) and FURLS Export Certificate Validation (FECV).

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 subject of this assessment is the Food and Drug Administration (FDA) Unified

Registration and Listing System (FURLS) and its component elements.

As part of FURLS, FDA created the FDA Industry Systems (FIS) to facilitate the making of submissions to the FDA, including registrations, listings, and other notifications. FIS is the portal for submissions. Submissions go through the Online Account Administration (OAA) application and into FURLS.

The FDA created the FIS and FURLS modules, in part, in response to the Bioterrorism Act of 2002, which gave high priority to improved information management to help protect the food supply. The Act requires that the FDA develop two systems: one to support the registration of facilities that manufacture, process, pack, or hold food products intended for consumption in the United States (Food Facility Registration or FFR) and one to receive prior notice before food is imported or offered for import into the United States (Prior Notice System Interface or PNSI). Under the law, the facilities had to be registered by December 12, 2003, when the "Prior Notice" requirement went into effect. FURLS maintains the OAA and FFR components, with OAA used to authenticate personnel who access to PNSI.
Since then, FDA has expanded FURLS to support the requirements of the following legislation:

Food and Drug Administration Amendments Act of 2007 -- Requires domestic and foreign device establishments to submit their annual establishment registration and device listing information to FDA by electronic means.

Food Safety Modernization Act (FSMA) of 2011 -- Greatly increased the authority of the FDA to regulate persons or groups who manufacture, process, pack, distribute, receive, hold, or import an article of food.

FURLS modules provide the capability for industry, both domestic and foreign, to register food, poultry, and medical facilities, request export certificates, provide product information, and apply to be added to listing programs. FDA manages these requests, communicates with industry, and approves

or rejects submissions through the FURLS modules.

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.	OAA is the FURLS user account database and user authentication module. Internal FDA users (employees and Direct Contractors) authenticate using Single Sign On (SSO). External users log into the system and authenticate (via username and password stored in FURLS) to determine which modules within FURLS the user can access per the users' access request. Users may be external (to FDA) industry users (local/foreign industry owners, operators, and agents) or state agency users under contract with the FDA. Users may also be internal (to FDA) such as permanent agency employees or FDA Direct Contractors. OAA collects the following personally identifiable information (PII) about external users: first and last name, state liaison email address (for state access), professional/office phone number and fax number, professional/office email address, professional/office mailing address, access credentials (username/password), and job title (potential PII if unique). The username is assigned by the system using the facility name and a random multi-digit number. The password is created by the user while establishing the FURLS account and is encrypted and stored within FURLS. For a listing of all FURLS modules/components, please see attached OC FURLS PIA, dated 12-1-2021. CECATS, CDER eCATS, CFSAN eCATS, CVM eCATS and BECATS also collect some non- PII data consisting of company taxpayer identification number (ID). The company Tax ID Code/Employer Identification Number (EIN) is only associated with CECATS, CDER eCATS, CFSAN eCATS, CVM eCATS and BECATS external users. Non-PII such as company tax ID, facility data and/or product information is collected in all FURLS modules as needed. Registrants may voluntarily submit additional non-PII data consisting of seasonal start/end dates or establishment type.
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	FURLS is a web-based system that allows foreign and domestic facilities to register with the FDA. It supports the implementation of FDA regulations that require facilities manufacturing, processing, or holding any FDA regulated products to register with the FDA. Most FURLS users are industry account holders who utilize FURLS to register their food, medical device, or poultry facilities. The remaining FURLS users are FDA employees and Direct Contractors who use the system to access facility registration information. Industry account holders access FURLS via web-based authentication using username and password which is managed at the database level. FDA employees and Direct Contractors access FURLS via a network-level SSO process using multi-factor authentication. FURLS consists of two types of modules: the web-based modules employed by users, and system support modules. The web-based modules are broken down by FDA components (aka Centers) and include: For information on each of the detailed modules, please see the attached OC FURLS Privacy Impact Assessment (PIA) dated 12-1-2021. FURLS users who access or use the system do not use any personal identifiers to retrieve records held in 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 Mother's Maiden Name E-Mail Address Phone numbers Taxpayer ID Mailing Address Others - a) Access credentials for external users (username/password) (b) fax number (c) All contact information is professional/office contact information only. The taxpayer ID is EIN of a company, not SSN.

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
PIA - 4:	For what primary purpose is the PII used?	The primary purpose of the PII in FURLs is to create, manage, and communicate regarding registrations/listings/certificates and associated industry users registering through FURLS. For example: username/password is used to ensure controlled, secure access; email and mailing address are used to communicate with industry users regarding any actions taken on submissions including new account creation, account deactivation or reactivation, temporary passwords for password reset, new submissions, status changes, return for action, and other actions.
PIA - 6:	Describe the function of the SSN/Taxpayer ID.	Taxpayer ID / Company EIN is collected for industry users registering through FURLS
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	FDA issues export certificates under Sections 801(e) or 802 under the Export Reform and Enhancement Act of 1996. Sections 510 and 905 of the Food, Drug and Cosmetic Act (FD&C, codified at 21 U.S.C. 360 and 387e) require establishments (e.g., manufacturers, re-packers, and re-labelers) to register with FDA upon engaging in the manufacture, preparation, propagation, compounding, or processing of FDA regulated products including food, drugs, medical devices, poultry, and biological products, with certain exceptions. Statutory citations: 21 U.S.C. 321, 331, 342, 344, 351, 352, 355, 360, 360b, 371, 374, 381, 387e, 393; 42 U.S.C. 262, 264, 271. 5 U.S.C. 301
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Email

		Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign 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.	Form 2541/2541d/2541e/2541f/2541g OMB Approval Number 0910-0037 OMB Expiration Date 10/31/2023 For additional OMB information collection approval #'s, please see attached OC FURLS PIA dated 12-1-2021.
PIA - 9B:	Identify the OMB information collection expiration date.	6/30/2022
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	State or Local Agency/Agencies Within HHS
PIA - 10A (Justification):	Explain why (and the purpose) PII is shared with each entity or individual.	Within HHS: FDA only. FDA's Office of Regulatory Affairs (ORA): ORA personnel who operate their FDA Inventory of Data Assets (FIDA), Import Trade Auxiliary Communication System (ITACS) and Prior Notice System Interface (PNSI**)** have restricted read access to some of the tables of the Food Facility Registration Module (FFRM)/Shell Egg Registration Module and have access to Online Account Administration (OAA) account information via Web Service call. State or Local Agency/Agencies: Personnel of State Agencies are Direct Contractors with the FDA who are provided read access to Food Facility Registration (FFR) data.
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)).	FDA establishes Memoranda of Understanding (MOUs) and employs Non-Disclosure Agreements to govern recipient data handling.
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	Facility/Registrant points of contact self-submit PII (work contact information)

		and are aware of the purpose of the FDA's use of the data for communicating with the submitter regarding a registration submission. All submitters may view additional information on FDA's privacy policies permanently posted on FDA.gov. At the time of hire, FDA personnel consent to the submission and use of their information by HHS/FDA as a condition of employment. HHS and FDA representatives, and the various individuals involved with the specific personnel data collection and use (such as Human Resources staff) provide notification to the subject personnel at the time the data is requested. Information that is provided about an individual is as it relates to their role in an organization instead of their personal information. At network logon all personnel and Direct Contractors must view and acknowledge a displayed text box warning advising there should be no expectation of privacy when using a government system. This PIA provides additional 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	There is no opt-out process for this system. Regulated entities are required by law to register and to submit information necessary to administer the registration process. FDA personnel and Direct Contractors consent to the submission and use of their information by HHS/FDA as a condition of employment. Personnel who opt not to provide PII would not be able to perform their assigned duties and maintain employment in their position.
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 FDA should change its privacy practices or its collection, use, or sharing of PII data in FURLS, the agency will notify the individuals whose PII is in the system in

		the most efficient and effective form available and appropriate to the specific change(s). This may include establishing a formal process involving written and/or electronic notice. Alternatively, the FDA will notify by informal processes such as e-mail to the affected individuals and/or FDA-wide e-mail blast.
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	External submitters (e.g., registrant point of contact) may contact the FDA offices identified in the FDA's online web/privacy policy and elsewhere on FDA.gov. They may contact FDA's Privacy Office directly. FDA personnel may raise concerns through the FDA Employee Resource and Information Center (ERIC) or contact FDA's Systems Management Center (SMC) or Privacy Office. All personnel are required to quickly report suspected breaches of PII 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	Registrants point of contact PII is self-submitted and registrants/facilities certify accuracy of information. Registrant points of contact may correct or update their information using FURLS, the contact information provided on fda.gov and/or the specific fda.gov web pages associated with the FURLS program. Accuracy is ensured by individual review at the time of reporting. Users may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Relevance of PII is ensured through the design of the system and modules to collect only PII elements necessary for the purposes of the system. 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. FURLS also performs quarterly review (UAR) of all internal FDA 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 Others

	Provide the reason of access for each of the groups identified in PIA -17	Users: FDA internal users and Direct Contractors receive, review, manage and track submissions. Administrators: Administrative purposes such as activating or re-instating a canceled facility registration and resetting passwords. Some of the administrators are Direct Contractors. Contractors: To view data in read only mode. Direct contractors require access to fulfill responsibilities under their FDA contract. Others: External/industry users can create their own accounts and submit data. The external users can only access their own PII data.
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	Personnel who have access to PII are provided the information based on the need for access required to perform their duties. Personnel who require access to the system must obtain supervisor approval and sign off before access is granted.
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 requesting user's supervisor will indicate on the account creation form the minimum information system access that is required for the user according to their role. The agency reviews the system access list on a quarterly basis and adjusts users' access permissions and removes unneeded accounts 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 FURLS users 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 by all FDA employees and Direct Contractors.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	FDA personnel who use FURLS receive FURLS-specific training on how to use the system and adhere to agency security, privacy, and other relevant policies. Privacy program materials are also available to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA. Privacy guidance is also available via the 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)	The agency continuously reviews the retention and destruction process associated with the information contained within FURLS to ensure it complies with FDA and NARA regulations. Applicable records control schedule: FDA file code 7210 and 7222 for Registration and Listing files and system database records; NARA approved citation N1-88-07-2. Disposition: Temporary - Cutoff after establishment goes out of business or product is not commercially marketed. The certificate modules delete/destroy after 5 years. All other modules delete/destroy 10 years after cutoff or when no longer needed for legal, research, historical or reference purposes, whichever is the latest. If data are migrated into a new system or replaced by a successor system, delete/destroy it after the verification of successful data migration. From the LACF PIA: FDA file codes 7220-7225 (NARA approved citation nos. N1-88-07-2 and General Records Schedule 20-2a, 2b, 4-7, 12, 16) cover FDA's Registration and Listing Systems. These files are temporary and are destroyed when no longer needed, the establishment goes out of business, the product is no longer marketed, Destroyed 10 years after cutoff.
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.
PIA - 25:	Describe the purpose of the web site, 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	FURLS is FDA's one-stop public web portal that allows FDA regulated industries to

		create and submit their submissions to the FDA via the internet. Examples of online submissions include registrations of establishments, listing of products, applications for export certification, applications for Accredited Third-Party certifications, and biological product deviation reporting. The general public can access front page of the website, but it is mainly used by industry to make submissions to the FDA and an account and password is required to log into the system.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	No
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No