PTA / PIA: FDA - DRLM - QTR2 - 2026 - FDA5270066

Created Date: 5/13/2026 6:21 PM Last Updated: 5/29/2026 6:17 PM

General Information

PTA / PIA Name:	FDA - DRLM - QTR2 - 2026 - FDA5270066	**PTA / PIA ID:**	4482095
Component Name:	FDA - OC Device Registration and Listing Module	**ATO Boundary Name:**	OC FDA Unified Registration and Listing System
Overall Status:	Complete	**# of Days - Open:**	25
Submitter:		**Submit Date:**	5/6/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
Office:		**OpDiv:**	FDA
Security Categorization:	High		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	7/11/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Anna Zhang
PTA 01A:	POC Title and Organization	Program Manager ODT/OIMT/OTD/DAS/EAB
PTA 01B:	POC Email Address	anna.zhang@fda.hhs.gov
PTA 01C:	POC Phone Number	240-447-5198
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The Food and Drug Administration (FDA) has made no changes to this system since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Bioterrorism Act of 2002 required the Food and Drug Administration (FDA) to develop two systems designed to safeguard the nation's food supply: 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). FDA implemented key provisions of the Act with the creation of the FDA Industry System (FIS, assessed separately) and the FDA Unified Registration Listing System (FURLS), a portfolio of registration, listing, export certification, reporting, and user authentication applications. These systems were created, in part, to streamline and modernize how FDA manages registration and listing information for the industries it regulates. The subject of this assessment is the Office of the Commissioner (OC) Device Registration and Listing Module (DRLM) application. OC DRLM allows foreign and domestic facilities to register with the FDA and maintain listings of the medical devices they manufacture, in accordance with requirements specified in the Code of Federal Regulations (CFR). The purpose of OC DRLM is to collect and maintain information regarding all facilities that manufacture medical devices and, for each facility a listing of each product manufactured at the facility. The system's primary functions include registering medical device establishments, maintaining an inventory of devices produced at each facility, and enabling secure communication between the FDA and industry users. Most OC DRLM users are industry account holders who access the system via web-based authentication using a username and password to submit and update registration and device listing information. The remaining users are FDA permanent employees and direct contractors who access the system via network-level single sign-on (SSO) with multi-factor authentication to review and manage facility registration and device listing information. OC DRLM maintains both personally identifiable information (PII) for user authentication and contact purposes, as well as non-PII such as facility names, establishment types, registration numbers, business activities, and device listings. This information is collected, maintained, and shared to support regulatory oversight, compliance monitoring, and public reporting when appropriate.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	OC DRLM is used to collect and maintain information regarding facilities that manufacture medical devices. The system maintains establishment registration records for these facilities and supports regulatory oversight by maintaining an inventory of registered

		establishments. In addition, for each registered facility, DRLM collects and maintains a listing for each medical device product manufactured, processed, or distributed by that facility including associated regulatory identifiers and device information. OC DRLM collects and maintains minimal PII about Internal users of the system component. FDA employees and direct contractors access OC DRLM using SSO with multi-factor authentication. For internal users, the system maintains only the information necessary to support access and regulatory oversight, including account credentials and minimal PII (email address and name) required to authenticate and manage users. This information allows FDA personnel to access facility registration and device listing data, perform regulatory review, monitor system activity, support auditing, and ensure accountability. Internal users do not rely on personal identifiers to access or retrieve records. OC DRLM also collects PII from external users who access the system to perform establishment registration and device listing activities. The PII collected includes the user's first and last name, mailing address (business), state liaison email address for state access (when applicable), phone number (business), fax number, and email address (business). The system also collects access credentials used to authenticate users. Usernames are automatically assigned by the system using the facility name combined with a randomly generated five-digit number. Passwords are encrypted and securely stored within DRLM. This information is used to manage user accounts, authentication access to the system, and enable regulatory communication related to device registration and listing activities. In addition to PII, the system collects and maintains non-PII information necessary for regulatory oversight and device tracking. This includes facility or product information required for device registration and listing. Registrants may also voluntarily submit additional non-PII data consisting of seasonal start and end dates or establishment types. This information supports the registration of medical device manufacturing facilities and the listing of product manufactured at those facilities. Note that any device identifiers included in general device information may become PII when combined with other PII. Records maintained in the system are retained in accordance with applicable National Archives and Records Administration schedule requirements and FDA policies.
PTA 05A:	Are user credentials used to access the system?	Yes

PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address HHS Username Password Non-HHS User Credentials Username Password

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	OC DRLM allows foreign and domestic facilities to register medical devices with the FDA. OC DRLM supports FDA regulations requiring facilities that manufacture, process, or hold FDA-regulated devices to register and list the devices they produce. Registered industry account holders access OC DRLM via web-based authentication using a username and password managed at the database level. The system collects PII from industry users including first and last name, mailing address (business), state liaison email address (business) (if applicable), phone number (business), fax number, and email address (business). OC DRLM also collects access credentials, including username and a password encrypted and securely stored within OC DRLM. This information is collected to authenticate users, provide secure access, facilitate regulatory communication, and ensure accountability for registration and device listings activities. External users do not use personal identifiers to retrieve records from the system. FDA employees and direct contractors access OC DRLM via network-level SSO with multi-factor authentication. The system maintains only account credentials (username) and minimal PII (name, email) about these users. This information is necessary to support access management, regulatory oversight, and user access to information required to perform their job duties Internal users do not rely on personal identifiers to access or retrieve records. OC DRLM also collects non-PII data necessary for facility registration and device listing, including facility names, establishment types, registration numbers, business activities, and for each facility a listing of each medical device manufactured. Registrants may voluntarily provide additional non-PII data, such as seasonal start and end dates or additional establishment type information. This data is collected to maintain an accurate inventory of medical device establishments and devices, support regulatory oversight, monitor compliance, facilitate reporting and analyses, and when appropriate share publicly available information. All information in OC DRLM, both PII and non-PII, is retained in accordance with FDA and National Archives and Records Administration (NARA) retention schedules to ensure availability for regulatory oversight, historical reference, auditing, compliance monitoring, and accountability, and is not retained beyond the period necessary to fulfill these purposes.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes

PTA 08A:	Provide the URL(s).	https://www.access.fda.gov/ This will take users to the FURLS OAA login screen, where once they are logged in, they are directed to DRLM.
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
PTA 09:	Describe the purpose of the website, 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.	The objective of OC DRLM is to support FDA regulations that require all medical device-related facilities or FDA-regulated medical products to be registered with the FDA in order to legally market products in the United States. FDA personnel can use the system to identify facilities not in compliance with FDA laws and regulations for firms manufacturing medical devices in the U.S. The website provides an additional way for external users to ensure they are in compliance with FDA registration requirements and enables FDA personnel to monitor domestic product status. Internal and external users access the system via public URL using different authentication processes. Internal users authenticate using SSO, while external users authenticate using username and password.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Device Identifiers Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other

PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Other: fax number; device identifiers may be collected as part of larger collection about device information.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	The PII collected in OC DRLM is used primarily to create and manage industry user accounts and to facilitate secure system access and related business communications. This includes using usernames and passwords to ensure controlled, secure access to the system, and using contact information (such as email and mailing address) to communicate with users regarding registrations, listings, certifications, submissions, account status changes (e.g., creation, deactivation, reactivation), password resets, and other actions associated with their submissions.
PIA 26:	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 28:	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: The Food and Drug Administration (FDA) may issue export certificates under sections 801(e) or 802 of the Federal Food, Drug, and Cosmetic Act (FD&C Act) (as amended by the Export Reform and Enhancement Act of 1996) to facilitate export of certain regulated products. Sections 510 (21 U.S.C. 360) of the FD&C Act require domestic manufacturers, re-packers, and re-labelers (and certain foreign establishments) of human or veterinary drugs and devices to register with FDA and submit product listings, when they engage in the manufacture, preparation, propagation, compounding, or processing of such regulated products, subject to certain exemptions. For food facilities, registration is required under section 350d of Title 21. 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.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No

PIA 30:	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 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	Form 3673 OMB Approval Number 0910-0625 OMB Expiration Date 4/30/2029
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	State or Local Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Within HHS: FDA only. FDA's Office of Inspections and Investigations (OII): OII personnel who operate their Firms Master List Service system (FMLS) have restricted read-only access to specific tables of OC DRLM. State or Local Agency/Agencies: Personnel of State Agencies are direct contractors with the FDA who are provided read-only access to OC DRLM data.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), 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 32D:	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.	OC DRLM does not have procedures for logging, tracking, or accounting for the sharing or disclosure of PII, because the Privacy Act does not require agencies to maintain an accounting of disclosures made for official work purposes within the Agency.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	For industry personnel (external users of the system) the submission of their PII is voluntary. The voluntary nature of account registration associated with OC DRLM serves as implicit consent, as individuals choose to provide the information to FDA in order to use the system. Individuals have the option not to submit information if they choose not to provide their PII, though this may prevent user access to the system. There is no method for employees to opt out of submitting their PII. Permanent employees, direct contractors, fellows, and other personnel must provide their PII for the agency to process administrative materials and securely administer access to agency information and property.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	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 notice on an FDA web site, email notice to the individuals, inclusion in newsletters, or information provided to supervisors with instructions to further inform staff. However, no such changes that would affect the rights or interests of the individuals are anticipated.
PIA 36:	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 individuals (registered industry account holders) who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system, or inaccurate, may contact the specific FDA offices to which they submitted their information and request correction of information or raise concerns about its use or disclosure. These offices can facilitate corrections to contact information or address concerns about how the information has been handled within the regulatory review process. These individuals may also contact FDA's Privacy Office using information provided on FDA.gov and FDA's intranet. The Privacy Office serves as a central resource for privacy-related concerns across all FDA systems and can assist individuals in understanding their rights, investigating concerns about inappropriate use or disclosure of PII, and facilitating resolution of privacy issues. FDA personnel may resolve such concerns by contacting the appropriate supervisor, system administrator, FDA's Employee Resources and Information Center (ERIC) or the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). In the event of a suspected incident or data breach, FDA personnel must rapidly report that without delay to the FDA's CIOCC.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	PII is provided voluntarily by the individual. They are responsible for providing accurate information. Industry account holders may submit a correction request to FDA to update their PII in the system. FDA relies on its personnel to ensure the accuracy and integrity of the information entered into these applications. FDA personnel are responsible for providing accurate information and may independently update and correct their information at any time. FDA provides avenues to ensure all information is as complete, accurate, timely, and relevant as possible. Accuracy is ensured by individual review at the time of reporting. 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 authorization 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.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: FDA employees require access to PII about themselves and other users to make proper annual updates. Allowing them to receive, review, manage, and track submissions. The PII is self-submitted, and registrants/facilities certify the accuracy of the information provided. External/industry users can create their own accounts and submit data. The external users can only access their own PII data. Administrators: Administrators require access to users' PII to perform essential administrative functions, including conducting annual updates, activating or reinstating canceled facility registrations, and resetting user passwords. A subset of these administrators are direct contractors. Contractors: To view data in read only mode. Direct contractors require access to fulfill responsibilities under their FDA contract.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users who require access to the application need to have supervisor approval and sign off before access is granted. The user's supervisor will use an account creation form to specify the minimum application access that is required for the user to complete his/her job. The agency reviews the access list for the application on a quarterly basis to review and adjust users' access permissions, and to remove unnecessary accounts from the application.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All system users at FDA complete mandatory annual 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 Digital Transformation (ODT) verifies that training has been successfully completed.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	FDA personnel who use FURLS receive FURLS-specific training (which includes OC DRLM) on how to use the system and adhere to agency security, privacy and other relevant policies. All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the agency's privacy office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.

PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (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. 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.
PIA 45:	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 training and awareness provided for all users; system manuals that advise on the systems' proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multifactor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the NIST’s Special Publication 800- 53 as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/8/2026
Privacy Analyst Review Comments:	Note the Archer error associated with question General 03: “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” The FDA instance of Archer is automatically entering the answer “No” which is incorrect. At this time, we are unable to update Archer to reflect the correct answer “Yes.” The ATO date is 7/11/2025. The FDA Archer Team is aware of this occurrence and is working on a solution.	**# of Days - PA Review:**	2

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/13/2026
SOP Review Comments:	The FDA’s Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls. 5.13.26	**# of Days - SOP Review:**	5

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/18/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 5/18/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	5

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	11

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 2:52 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				