PTA / PIA: FDA - MRCD - QTR4 - 2025 - FDA4995881

Created Date: 10/30/2025 12:40 PM Last Updated: 1/21/2026 11:36 PM

General Information

PTA / PIA Name:	FDA - MRCD - QTR4 - 2025 - FDA4995881	**PTA / PIA ID:**	3953309
Component Name:	FDA - CDER Mercado	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	21
Submitter:		**Submit Date:**	10/30/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
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)?	Yes
General 04:	ATO Date or Planned ATO Date.	5/26/2025
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	Venu Boppana
PTA 01A:	POC Title and Organization	Senior Operations Research Center for Drug Evaluation and Research (CDER) Office of Business Informatics (OBI)
PTA 01B:	POC Email Address	venugopal.boppana@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-0977
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.	Since this Privacy Threshold Analysis/Privacy Impact Assessment was last approved, FDA made the following changes to Mercado: in the last PIA, Mercado was documented alongside Panorama. Panorama has been replaced by another application and Mercado is the only subject now covered under this assessment.
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 Food and Drug Administration (FDA) uses the Center for Drug Evaluation and Research Regulatory Review (CDER RR) system for tracking, reporting, and maintaining an archival record of the drug and biological product materials submitted to the FDA for review. CDER reports to Congress on a number of issues, including performance on Prescription Drug User Fee Act (PDUFA) related goals. CDER also uses data in RR for reporting purposes. This assessment addresses CDER Mercado, one application operating within the CDER RR system boundary. Other CDER RR applications/components are addressed in separate assessments. CDER Mercado improves the ability of individuals to review and analyze CDER's regulatory science and regulatory management data. The Mercado system improves regulatory and scientific decision making, organizational performance, and the quality and consistency of data while supporting a self-service reporting environment. The Food and Drug Administration's Mercado system is a marketplace of data for all regulatory reporting and analytical needs across the Center for Drug Evaluation and Research (CDER). Mercado does not contain information but instead displays information such as application sponsor data (for abbreviated New Drug Applications (ANDAs)), inspections-related data, User Fee information and other similar information to support CDER inspectors, reviewers, and analysts. Mercado pulls the data from CDER's Document Archiving Reporting Regulatory Tracking System (DAARTS, addressed in a separate PIA) and the displayed information includes attachments that may contain (in open text fields) the names of individuals who are filing reports or describing drug effects (e.g., adverse events data from FDA's Adverse Event Reporting System (FAERS), the subject of a separate assessment). CDER's business practice (internal office procedures) is to anonymize, by manual review and redaction or removal of PII, text fields that could possibly contain PII. These practices are conducted on the source database systems where the information is kept for three-years. Users of the system are CDER personnel (FDA permanent employees and Direct Contractors) with assigned roles in the human drug review process. Access to Mercado for FDA employees and Direct Contractors is controlled by Single Sign-on (SSO) and requires use of the personal identity verification (PIV) card. No usernames or passwords for these applications are stored within CDER RR.

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.	CDER Mercado collects personally identifiable information (PII). PII in the system is collected for creation and maintenance of user accounts, and to facilitate user access to the system. PII about users includes name, business email address, and business phone number. The system also displays information that may contain PII and potential PII (e.g., adverse events reports) which may include name (company and individual point of contact), business/personal mailing address, business/personal phone number, and business/personal email address. Non-PII data available for review by users may include inspections-related data, trade secrets, and User Fee information. System information is maintained in accordance with National Archives and Records Administration (NARA) guidelines and schedules. PII data is not shared with any other Agency or outside organization.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory
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.	CDER Mercado collects PII about users of the system (FDA permanent employees and Direct Contractors). PII in Mercado consists of user information associated with account creation and system access. PII includes name, business email address, and business phone number. CDER Mercado also displays information that may contain PII and potential PII included with source system data (e.g., adverse events reports). Potential PII may include name (company and/or individual point of contact), business/personal mailing address, business/personal phone number, and business/personal email address. Non-PII data available for review by users may include inspections-related data, trade secrets, and User Fee information.
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).	Internal only Uniform Resource Locators (URLs) include: https://mercado.fda.gov/analytics https://mercado.preprod.fda.gov/analytics
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No

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 purpose of the Mercado website is for users to access reports available in the system. Only FDA employees and contractors have access to the system, and they must authenticate through SSO and use of PIV cards to access the system. Users access the system through internal URLs.
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.	Biographical Information Name Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of creating and maintaining user accounts for Mercado.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There are no secondary uses associated with CDER Mercado 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: Provisions of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 301, including sections 353, 355, 356b, 360 (regulated entities to provide necessary contact information to FDA); the Drug Supply Chain Security Act (DSCSA), 21 U.S.C. 581 et seq.; and Departmental regulations, 5 U.S.C. 301.
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 Online Government Sources Within the OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The Paperwork Reduction Act (PRA) requires an OMB information collection approval number if the system collects information from 10 or more persons other than Federal Employees. Mercado only collects information from Federal Employees and Direct Contractors and does not collect information on the public. As such, Mercado does not require an OMB information collection approval number.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
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.	Individuals may opt-out of the collection or use of their PII by not having a user account in Mercado. There is no option to object to or opt-out of the information collection if users wish to use the system. User accounts must be tied to an individual, per policy.
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.	While the FDA does not anticipate major changes to the type of PII collected/maintained in the system or how it is used, FDA will notify system users of any major changes to the system should they occur. 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 email to individuals, adding or updating online notices or forms, updating this assessment, or other available means to inform the individual.

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.	If the system contains incorrect contact information for a user, the account likely will not function correctly and system administrators would fix the issue. If a user notices incorrect information in their account, the user can contact system administrators to fix it. 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 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). In the event of a suspected incident or data breach, FDA personnel must rapidly report that without delay to the FDA's Cybersecurity and Infrastructure Operations Coordination Center (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.	FDA's Office of Information Security (OIS) performs user account validation quarterly. As part of this exercise, each account is validated for accuracy and the correct permission levels. Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. 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 Developers 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 can only access PII about themselves. Administrators require access to PII about users to administer and operate the system. Administrators of the system are contractors. Developers (also contractors) can only access PII related to accounts in the lower environments, not production. Access is required to maintain application. Contractors: Some administrators/developers are Direct Contractors.
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 information system need to have supervisor approval and sign off 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 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.	System administrators/developers require access to account information in order to manage and maintain the system. The relevant supervisor will indicate determine 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 using network and system level controls and settings to control access at the individual level.
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 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 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.	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 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).	Mercado follows NARA GRS. 3.2, Item 31, Systems Requiring Special Accountability for Access. TEMPORARY. Audit log files may be held for 6 years.

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.	Mercado utilizes single-sign-on for authentication, which requires use of a personal identity verification (PIV) card issued by the FDA. The system limits access to data to only those that have explicitly been granted access. Data is stored internally in the FDA's Ashburn Data Center. 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 multifactor 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.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	10/30/2025
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 5/26/2025. The FDA Archer Team is aware of this occurrence and is working on a solution.	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	10/30/2025
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. 10/30/2025	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/17/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/17/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	18

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/20/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/20/2025 11:03 AM	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				