PTA / PIA: FDA - eMDM - QTR2 - 2025 - FDA4919176

Created Date: 5/12/2025 8:30 AM Last Updated: 5/22/2025 4:38 PM

General Information

PTA / PIA Name:	FDA - eMDM - QTR2 - 2025 - FDA4919176	**PTA / PIA ID:**	3166426
Component Name:	FDA - OC Enterprise Master Data Management	**ATO Boundary Name:**	OC FDA Intelligent Data Lifecycle Ecosystem
Overall Status:	Complete	**# of Days - Open:**	21
Submitter:		**Submit Date:**	5/6/2025
Next Assessment Date:	05/21/2028	**Expiration Date:**	5/21/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
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.	5/13/2024
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	POC Name: Thomas Beach
PTA 01A:	POC Title and Organization	POC Title: Project Manager POC Organization: ODAR
PTA 01B:	POC Email Address	thomas.beach@fda.hhs.gov
PTA 01C:	POC Phone Number	202-748-6977
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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) Centers and Offices are largely served by disparate systems, both off-the-shelf and custom-made, and processes, which create conflicting results when reconciliation across data sources occurs. The FDA seeks to harmonize key master data through an enterprise approach and establish an Enterprise Master Data Management (eMDM) Practice for managing shared data across the Agency. The eMDM practice is aligned to realize organizational goals, reduce risks associated with data redundancy, ensure higher quality data, and reduce the costs of data integration and licensing. The eMDM Practice will address the following needs: • Create an Agency-wide standard for key entity data domains. • Enable easier exchange of information between systems. • Provide accurate and consistent data to all Agency constituents when and how required. • Establish clear data quality standards and metrics to assess on continuous basis.
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.	Firm registration information from multiple data sources is shared with eMDM. The firm registration information includes business/firm name, firm mailing address, point of contact name, point of contact phone number (if available) and point of contact email (if available), business activity type, Data Universal Numbering System (DUNS) number, and FDA Establishment Identifier (FEI). The eMDM data sources will include but may not be limited to: • Office of Inspections and Investigations (OII) - Firm Management Service (FMS) • Center for Biologics Evaluation and Research (CBER): Blood Establishment Registration (BER), Human Cell and Tissue Establishment Registration System (HCTERS) and Regulatory Management System - Biologics License Application (RMS-BLA) • Center for Drug Evaluation and Research (CDER) – CDEROne, Electronic Drug Registration and Listing System (eDRLS), Integrated Data Management (Integrity) • Human Foods Program (HFP) - Food Facility Registration Module (FFRM) • Center for Tobacco Products (CTP) – Addressbook, Tobacco Registration and Listing Module (TRLM), Next Generation (NG), and Product Management Service (PMS) • Center for Devices and Radiological Health (CDRH) - Device Registration and Listing Module (DRLM), Submission Entry Management (Centry) • Center for Veterinary Medicine (CVM) - Corporate Database Portal (CDP)

		• External – Google Geo Coding, and Dun and Bradstreet (D&B). The PII maintained in eMDM system is primarily used for work tracking, management, and communication. The PII maintained in eMDM is business point of contact information (contact name, mailing address (business), business phone number (if available), business email (if available)), and DUNS number. Non PII that is collected is FEI. eMDM does not determine the primary use of PII in the data sources. The source system teams, and their specific programs identify the primary use of PII for each individual system through system specific privacy assessments. The eMDM system will be accessed by FDA Full Time Equivalent (FTEs) and contractor team members. eMDM applications are integrated with Enterprise Single Sign-on (SSO). The users will be able to access the eMDM Products and Services User Interface (UI), E360, eMDM toolkit, Data Wrangling (Trifacta), FDA Data Market Place applications to search the FDA AddressBook, review dashboard reports and other pertinent information about the business/firm. The information is stored in accordance with the source system National Archives and Records Administration (NARA) requirements.
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.	Ping-Federate which is integrated with the 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.	eMDM serves as a repository of firm's data collected from other systems throughout the FDA and then maintained in a collective location in order to provide a comprehensive firms view that crosses Centers and systems. Firm's data includes FEI and DUNS numbers, firm's details like physical and mailing addresses, firm point of contact information (name, phone number (business), and email (business)) as identified via submission/source system or third-party data source system, and related products supported. The security architecture was designed to maximize security across the agency. Authentication is done through Alt-PIV card by Ping-Federate which connects to individual Active Directory groups from each center. Authorization of Admin accounts are done through Role Based Access Control (RBAC). Amazon Web Services (AWS) Single Sign on (SSO) supports automatic provisioning (synchronization) of user and group information from the PingFederate product by Ping Identity (“Ping”).

PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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 DUNS Biographical Information Name 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.	FDA Establishment Identifier (FEI)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100,000 – 999,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose of the PII is firms point(s) of contact name and contact information such as phone number and/or email address to follow up on business communications.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Legal authorities governing information use and disclosure specific to the system and program are: 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 301, including sections 353, 355, 356b, 360 and 379k
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.	Government Sources Within the OPDIV Non-Government Sources Commercial Data Broker

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.	This system/component does not collect information using an information collection request as defined by the Paperwork Reduction Act.
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.	There is no option to object to or opt-out of the information collection because PII in eMDM is derived from other agency applications/systems and a commercial data broker rather than collected from data subjects directly. Thus, the mechanism for information collection is adopted from the source system and/or third-party data supplier and an additional opt-out mechanism is not applied.
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.	No such changes are anticipated for the eMDM system. If FDA changes its practices regarding the collection or handling of PII related to eMDM, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII.
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.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have several avenues of recourse available. These individuals may contact FDA officials via email, phone and standard mail (all listed on fda.gov and the agency's intranet). Offices available to assist include FDA's Employee Resource Information Center (ERIC Helpdesk), the Cybersecurity Infrastructure Operations Coordination Center (CIOCC) (security incidents, privacy breaches), and FDA's Privacy Office (concerns, complaints, possible breaches).
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.	The eMDM system does not conduct periodic reviews of PII as it does not directly collect data related to users or any group of users. Satisfying periodic review requirements and ensuring accuracy and relevancy of the data is the responsibility of System Teams and their specific programs. Integrity and availability of data in eMDM are protected by security controls selected and implemented while 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 - Users will have access to PII to review and manage the application. Note that "users" may include supervisors or system administrators. Administrators - System administrators may have access to PII to conduct business functions. System administrators may have access to PII to support system administration activities. Developers - Developers may have access to PII to maintain the system and provide technical assistance to users. Contractors - Some Direct Contractors are developers and system administrators that support users.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures in place to determine which system users may access PII are: Access to eMDM is based on role-based access control (RBAC), need-to-know and least privilege. System accounts are reviewed on a regularly basis to determine if access is still required for each user.
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.	User privileges and access controls for eMDM are set based on each user's specific role, administrators versus developers, within the eMDM environment. The relevant Full Time Equivalent (FTE) supervisor will indicate on the eMDM user account list the minimum access that is required for the user to complete their job. Based on role-based criteria and using technical settings/controls, the scope of access is restricted to match the individual's role and related need for data access.
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 FDA users of eMDM 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 individuals successfully complete training.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	There is no additional training specific to eMDM training above and beyond eMDM users security and privacy awareness training. However, FDA Employees and Direct Contractors are trained on the Rules of Behavior, and conduct system-use knowledge sharing within the user group.
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).	FDA maintains the records in eMDM in accordance with National Archives and Records Administration (NARA) approved Citation GRS 5.2, Item 020, Intermediary Records. Disposition: TEMPORARY. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
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 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.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/6/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/12/2025
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.	**# of Days - SOP Review:**	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/19/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/19/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	7

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/22/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/22/2025 12:01 PM	GUENTHER, BRIDGET	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
PTA 04	BLAND, CRYSTAL	5/19/2025	In the next iteration of the PTA please remove the bullets, they're not 508 compliance.	