PTA / PIA: FDA - LDD - QTR3 - 2025 - FDA4949795

Created Date: 8/4/2025 8:41 AM Last Updated: 8/5/2025 4:42 PM

General Information

PTA / PIA Name:	FDA - LDD - QTR3 - 2025 - FDA4949795	**PTA / PIA ID:**	3598926
Component Name:	FDA - CBER Lot Distribution Database	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	4
Submitter:		**Submit Date:**	8/1/2025
Next Assessment Date:	08/04/2028	**Expiration Date:**	8/4/2028
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)?	No
General 04:	ATO Date or Planned ATO Date.	11/21/2022
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	Christopher Kiem
PTA 01A:	POC Title and Organization	System Owner FDA/CBER
PTA 01B:	POC Email Address	Christopher.Kiem@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-8093
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 the Center for Biologics Evaluation and Research (CBE)R Lot Distribution Database (LDD) component since the last Privacy Threshold Analysis/Privacy Impact Assessment 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.	A vital part of the mission of the Center for Biologics Evaluation and Research Office of Biostatistics and Epidemiology's Division of Epidemiology (CBER/OBE/DE) is the post-marketing surveillance of biological products. For vaccine and therapeutic (including blood and blood products) safety evaluators, lot distribution data is important in safety surveillance for detecting potential problems associated with unusual concentrations of a particular adverse event in one or more production lots for individual CBER-regulated products. Lot distribution data is also important in emergencies where products need to be recalled, since lot distribution data provide a means for tracking the national supply of products. Data cross-reference between Lot Distribution Database (LDD) and Vaccine Adverse Event Reporting System (VAERS) provides viable information for tracking vaccine doses distributed by manufactures. The CBER Office of Regulatory Operations (ORO) system exists to provide a central location to collect, review, and analyze Adverse Event Reports for all CBER regulated products. Each component of the CBER ORO system which are covered in their own Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA), captures different information from different data sources. This assessment focuses on the CBER Lot Distribution Database (LDD) component. The LDD is used to track specific lots of biologic products so that they may be included as part of an adverse event review, or to enable recalls if needed. LDD Data is received through the FDA Electronic Service Gateway (ESG) (which has its own PIA) direct from manufacturers in Structure Product Label standardized format (established and maintained by an organization known as Health Level 7 (HL7)).

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.	LDD collects PII data that consists of adverse event reporters' contact information that includes name, phone number (personal/business), mailing address (personal/business), email address (personal/business), and the reporter's date of birth. LDD also contains non-PII data that is used primarily to analyze biological products distribution and for the cross-reference with VAERS and CBER Adverse Event Reporting System (CBAERS) data. VAERS and CBAERS are covered in separate assessments. All data collected in LDD is accessed through the CBER ORO System. The CBER ORO System is provided to users "as-is" in that it shares information that it has received from other source systems but does not create or modify any data it contains. Information about the users themselves (the medical reviewers, systems administrators) are managed through network access protocols and all have FDA system access credentials. All users are authorized FDA network users and only have access via single sign-on. Access to this system is granted through the CBER Menu application with single sign-on. All users of the system are FDA Employees and Direct Contractors with FDA badges and Personal Identity Verification (PIV) cards. LDD Data is stored in a secure relational database and is retained according to the applicable records retention policy (identified later in this document).
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.	The Lot Distribution Database (LDD) is the post-marketing surveillance application for detecting potential problems associated with unusual concentrations of a particular adverse event in one or more production lots for individual CBER-regulated products. Per regulation, information on biologic products released through distribution channels in the US is sent periodically to the FDA. This information is entered into an automated system where available electronically and filed as hard copy where not available electronically. LDD data is used primarily to analyze biological products distribution and for cross-referencing with VAERS and CBAERS data. LDD is also important in emergencies where products need to be recalled, because lot distribution data provide a means for tracking the national supply of products.
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://cberforms.fda.gov/forms/frmservlet?config=cber&form=ldd_inbx
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.	LDD is the post-marketing surveillance application for detecting potential problems associated with unusual concentrations of an adverse event in one or more production lots for individual CBER-regulated products. The website provides FDA Employees and Direct Contractors access to LDD data that is used primarily to analyze biological products distribution and for the cross-reference with VAERS and CBAERS data. LDD is also important in emergencies where products need to be recalled, since lot distribution data provide a means of tracking the national supply of products. The LDD application is internally accessed through the CBER ORO System. The CBER ORO System is provided to users "as-is" in that it shares information that it has received from other source systems but does not create or modify any data it contains. Information about the users themselves (the medical reviewers, systems administrators) are managed through network access protocols and all have FDA system access credentials. All users are authorized FDA network users and only have access via single sign-on.
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 Date of Birth 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 Patients Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	1,000,000 or more
PIA 25:	For what primary purpose is the PII used?	The information (if provided) is used to contact people to clarify data regarding their submissions and to assist in follow-up analysis of the data.
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 Provisions of the Food, Drug, and Cosmetic Act, 21 U.S.C. 301, including sections 353, 356b, 360; Public Health Service Act, 42 U.S.C. 201 including sections 262, 263a.
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).	Medwatch Form 3500 (used by FAERS information source for CBAERS): OMB No. 0910-0291, Expires: 7/31/2028

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.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	The PII is shared and disclosed with CDER and the Center for Decease Control (CDC) for joint handling of adverse events regarding vaccines.
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)).	Interagency agreement with CDC, IAG # 224-08-1093. This joint agreement stems from a joint FDA-CDC project required under the National Childhood Vaccine Injury Act (NCVIA), P.L. 99-660.
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.	Data is not disclosed outside of the Department of Health and Human Services (HHS). Personnel requiring access are provided with disclosure accounting guidance and resources, however, these applications are not subject to the Privacy Act, and its requirement to maintain an accounting of certain disclosures.
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.	HHS and FDA personnel that use the systems are notified, and as a condition of employment and use of the systems, consent to the use of their information by FDA and HHS at the time they are hired. Voluntary Reporters are not required to report PII of the affected individuals, and have full control over the submission of PII, if any. Mandatory reporters (e.g. manufacturers) do not have a choice regarding the submission of information including PII about themselves. This information is essential for FDA to effectively analyze and respond to event reports and thereby protect against unsafe biologic products in the marketplace. However, those mandatory submissions are made to systems maintained by the CDC and FDA CDER, and the collection of that information is addressed in PIAs for those other systems. PII about the individuals affected by adverse events is not required and is not expected to be reported. Information provided (adverse event experienced, dates of events, relevant health conditions) is not sufficient to identify the individual, alone or in combination with other reasonably available information.

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.	PII data maintained in CBER ORO is obtained directly from CDC's VAERS and FDA's FAERS. Operators of those systems are responsible for notifying the individuals of any changes to the collection or distribution of PII data. LDD PII data consists of the reporters' contact information only, and changes to the LDD system are communicated to its users through the CBER LDD Coordinator. This may include a formal process involving written and/or electronic notice, or informal processes such as e-mail notice to the individuals.
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 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 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.	Reporter's PII is provided voluntarily by the individual. 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. 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 security controls selected and implemented during providing the system with an authority to operate (ATO). Controls are selected based on the 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. CBER performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered.
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 require access to full AERS to analyze adverse events data. Administrators: System administrators require access to users account information to conduct system maintenance and provide quality control. Developers: Developers may have access to user or AERs subject PII incidentally to unit and system testing and development. Contractors: Some system administrators or developers may be Direct Contractors and will have access to PII under the same circumstances as FDA employees in those roles.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature 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.	All users including administrators, developers, and Direct Contractors are granted only the minimal privileges that they require to do their job. The users' supervisor indicates on the account creation form the minimum system access that is required. All users are FDA network users and must have a current Personal Identity Verification (PIV) compliant badge.
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.	System users receive system-specific training, review the HHS 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).	All adverse event files are temporary, and destroyed according to the instructions cited in the following records schedules: FDA 5, Adverse Event/Experience and Product Defect Reports; 5.1 Adverse Event Management Files; 5.2 Adverse Event Reports or Forms; 5.3 Adverse Events Reporting Systems; 5.3.2 AERS Database Records; 5.3.3 Extracts of the Adverse Data for Public Access; Output Records; General Records Schedule (GRS) 3.1, item 051 Disposition: Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use. GRS 4.3, Items 010, 011, 012, 020, 30, and 31. Disposition: Temporary. Destroy when business use ceases. CBER Records Control Schedule (NARA Schedule No. N1-088-03-05) Items B-34, Post Marketing Products Safety Reviewers and Adverse Event Summaries, and B-35 Post Marketing Surveillance Lot Analysis Reports. Records are retired to the Washington National Records Center three years after the cut-off date and destroyed 20 years after the cut-off date.
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:**	8/1/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/4/2025
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:**	3

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	8/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 8/5/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/5/2025
SAOP Review Comments:	Approved on behalf of the SAOP.	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/5/2025 12:49 PM	BLAND, CRYSTAL	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 01	BLAND, CRYSTAL	8/4/2025	8/4/2025 Per FDA's Email: The PIA is experiencing an Archer error with question General 03: "Does the system have or is it covered by a Security Authorization to Operate (ATO)?" o The FDA instance of Archer is automatically entering the answer "No," which is incorrect. The ATO date is 11/21/2022. o At this time, we are unable to update Archer to reflect the correct answer "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution	8-4-2025 EMAIL_PIA in Queue (CBER Lot Distribution Database).pdf CBER Lot Distribution Database PIA_SOP Approved.pdf