Privacy Impact Assessment (PIA): FDA - LDD - QTR2 - 2022 - FDA2041809

Date Signed: 5/9/2022

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1440163
PIA Name:	FDA - LDD - QTR2 - 2022 - FDA2041809	**Title:**	FDA - CBER Office of Regulatory Operations
OpDiv:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
PTA - 5A:	If yes, Date of Authorization	6/19/2018
PTA - 5B:	If no, Planned Date of ATO	6/18/2018
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	No changes made to the system since the last PIA approval.
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	This document addresses the Post Market applications within the Center for Biologics Evaluation and Review (CBER) Regulatory Management system. CBER Regulatory

		Management Post Market applications (RMS-PM applications) supports CBER post market safety surveillance and adverse event monitoring activities. The RMS-PM system contains patient, care provider, event reporter, and product data collected from other systems (with their own PIAs). The FDA Adverse Events System (FAERS) and Center for Decease Control's (CDC) Vaccine Adverse Events System (VAERS) are the primary data sources for the CBER RMS-PM System. These data sources are established and data is provided via system-level connections with the source systems at CDC (VAERS) and FDA's Center for Drug Evaluation and Research (FAERS). The data contained in the RMS-PM is refreshed daily; data is overwritten and updated with the latest available data from VAERS and FAERS. There are three sub-systems included in this RMS-PM assessment document, grouped together because they support post market product safety surveillance, handle similar data and are governed by similar controls and authorities.
PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The RMS-PM system exists to provide a central location to collect, review, and analyze Adverse Event Reports for all CBER regulated products. Each component of the RMS-PM system captures different information from different data

sources.

1. CBER Adverse Events Reporting System (CBAERS): Collects adverse event reports from the FDA Adverse Event System (FAERS, covered by its own PIA) and provides a user interface. Data is exclusively provided by the FAERS system through an electronic process that is updated daily. Information in CBAERS includes data that have been reported as part of an adverse event report (the nature of the adverse event, the product with which it is associated, the date when it occurred, the amount or dose involved, along with open fields to provide more information), along with information about the person making the report.

FAERS collects the following PII information: (a) name; (b) mailing address; (c) phone number; (d) e-mail address; and (f) date of birth.

FAERS also collects the following non-PII data: (a) occupation; and (b)the facility where the event takes place, and some identifying information about the patient ("patient identifier" which can be the person's initials or some other recognizable identifier including: (a)age; (b) sex; (c)weight; (d)race; (e) ethnicity; all of which is collected through the FAERS system. A query interface for the Lot Distribution Database (LDD) provides CBAERS the capability to query identifying information about lots (when that information has been provided).

CBAERS receives FAERS data from the Agency's Center for Drug Evaluation and Research (CDER) and transforms it into a searchable structure within its database. Users interact with CBAERS data through controlled business objects interfaces (require a valid FDA username/password/token combination for access). CBAERS also provides a nightly data extract to CDER's Empirica Signal data mining application (assessed in another PIA). This nightly extract provides CDER Medical Reviewers with data from CBAERS for their own review processes.

2. Lot Distribution Database: 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)).

3. CBER Vaccine Adverse Event Reports System: CBER VAERS receives information from the CDC VAERS, and provides CBER users with a means for performing analysis and ad hoc data querying of vaccine adverse events. Data includes information about vaccine adverse events that have been reported to the CDC, along with all the same information about the person making the report, the person experiencing the adverse event, and the time and location of the adverse event as are provided in CAERS. CBER VAERS also has an electronic submission process that allows manufacturers of vaccines to report directly to FDA concurrently with reports to CDC using the individual case safety report (ICSR) electronic submission format. These reports come in through the FDA ESG.

All data collected in the RMS-PM 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 either full time employees of the federal government, or are Direct Contractors with FDA badges and smart cards.

PTA -9A:	Are user credentials used to access the system?	Yes
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	1. CBER Adverse Events System: The CBER Adverse Events Reporting System (CBAERS) provides a means for analysis and querying of individual biologic adverse events in the FAERS systems. It also is a source of data for CBER and CDER data mining efforts. Besides FAERS, it also provides cross-reference interface to the Lot Distribution Data (LDD) application, Adverse Event Product Problem (AEPP) application, and to some of the data elements in RMS-BLA. PII Data that is submitted includes information about the patient as well as the reporter of the adverse event. Patient information is not required, but is sometimes voluntarily provided. Reporter PII is required to assist with follow up questions and information that may be needed as well as statistical analysis. Data is stored in a secure, relational database with user access controls, according to the appropriate records retention schedule. 2. Lot Distribution Database: 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. LDD Data is stored in a secure relational database and is retained according to the applicable records retention policy (identified later in this document). 3. CBER VAERS: The CBER VAERS system consists of adverse event reports associated with U.S. licensed vaccines submitted by health care providers, manufacturers, and the public. VAERS is populated with data from the broader joint FDA and Centers for Disease Control and Prevention (CDC) managed VAERS program, which allows both fixed-format and ad hoc analysis of individual vaccine adverse events, as well as aggregated adverse event cases. Information in VAERS is provided by CDC and is shared with CDER as a data extract file to Empirica Signal (a CDER system covered in a separate PIA) in support of wider post market surveillance.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No

PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name E-Mail Address Phone numbers Date of Birth Mailing Address
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Patients Public Citizens
PIA - 4:	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 - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	None.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	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 - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign Non-Government Sources Members of the Public Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	MedWatch Form 3500 (used by FAERS information source for CBAERS): OMB No. 0910-0291, Expires: 1/31/2025
PIA - 9B:	Identify the OMB information collection expiration date.	1/31/2025
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 10A:	Identify with whom the PII is shared or disclosed and for what purpose	Within HHS
PIA - 10A	Explain why (and the purpose) PII is shared with each entity or individual.	Information is shared with CDER and the Center for Decease Control (CDC) for joint handling of adverse events regarding

(Justification):		vaccines.
PIA - 10B:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	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 - 10C:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII	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 - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	FDA personnel and Direct Contractors who require access to the RMS-PM system are notified at the time of hire and when they request access to the system. FDA center representatives, and the various individuals involved with the specific data collection and use provide notification to the employees and non-employees at the time the data is requested. For specific PII that is sometimes provided in adverse event reports, this notice is provided at the time of collection directly from the system that has collected that information, which are maintained at the CDC and in the CDER Center and subject to their own PIAs. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet (https://www.fda.gov/about-fda/about-website/website-policies) pages. This PIA provides further notice.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	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 - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained	PII data maintained in RMS-PM 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. System updates to CBER VAERS and CBAERS systems are communicated to the users of those systems through system update notices and through the points of contact as needed for the CDC VAERs or CDER FAERS systems. 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 - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not	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 - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no	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

	processes are in place, explain why not	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 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 - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17 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 - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	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 - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	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 - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors	All system users at FDA take annual mandatory computer security and privacy awareness training. This training includes

	and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	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 - 21:	Describe 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 - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	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) 20, Electronic Records, Items 2a,2b,4,5,6,7, 11a(1), 12, 16. 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 - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.