Privacy Impact Assessment (PIA): FDA - ODW - QTR1 - 2022 - FDA2034572

Date Signed: 6/28/2022

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:**	1435967
PIA Name:	FDA - ODW - QTR1 - 2022 - FDA2034572	**Title:**	FDA - CDER Opioid Data Warehouse
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	8/7/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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?	The Food and Drug Administration (FDA) Opioid Data Warehouse (ODW) integrates over 30 disparate data sources into a centralized, secure,

		and scalable cloud environment to enable search, analytics, and reporting using custom built or Commercial off the Shelf (COTS) tools. Deployed within the Amazon Web Services (AWS) GovCloud environment, the ODW automatically ingests, processes, and stores over thirty diverse data sources within a unified environment. The ODW provides powerful applications/tools that enable enhanced data search, visualization, and analysis to support opioid regulatory decision making. Streamlined access to opioid data and advanced analytics within a single platform enables FDA personnel to better assess vulnerability points in the population; identify early trends that may be contributing to the opioid crisis; and target early regulatory changes to address the evolving opioid crisis. While the ODW is intended to provide an FDA enterprise wide capability, the current version contains applications/tools that specifically addresses the following user communities: (1) The Office of Compliance (OC), to proactively monitor and, when necessary, quickly and precisely respond to imports, recalls, shortages, and drug supply chain issues that may negatively impact patient safety and/or are candidates for surveillance and enforcement action; (2) The Office of Communications (OCOMM)., to enhance and automate social media analysis to understand themes, products, events, attitudes, and behaviors being discussed in online platforms; (3) The Office of Surveillance and Epidemiology (OSE), to investigate, summarize and display patterns and trends in opioid dispensing / administration, abuse and diversion, distribution, and morbidity and mortality; and (4) The Office of Strategic Programs (OSP), to access data source dictionaries and documentation to facilitate understanding of data characteristics and considerations, and improved coordination with OSE.
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 Opioids Data Warehouse (ODW) is a data warehouse that aggregates diverse data collected by other systems and provides analysis support for regulatory decision making. All data

in the ODW, including any personally identifiable information (PII) and data that might contain PII, is stored and/or archived indefinitely unless it is determined that the data is inaccurate and needs to be corrected.

While the ODW does not actively solicit, request, or collect any PII, data is ingested into the ODW that might contain or does contain PII:

1. Information about companies, including contact information for individuals acting in the representatives of their company,
2. Inspection data includes the name of a Firm & address as well as the names of individuals involved in the inspections (Lead Signatory and Supervisor). Free text fields may contain sensitive information about the details or outcomes of inspections.
3. The ODW ingests social media data, which may contain PII. Social media users can enter any kind of text in social media platforms (e.g. Reddit, Twitter). PII content is removed from social media data prior to ingestion into the ODW. However, comprehensive removal of all PII can present challenges because PII can exist in many formats that are not always distinguishable from other data. Some user first and last names may be included in the social media data, but not all user account information are able to be tied back to an individual. FDA uses the social media data to enhance analysis to understand the social context surrounding drug-related themes, products, events, attitudes, and behaviors being discussed in online platforms.
4. Data collected for OSE and OSP Contains PII - The ODW ingests data from the FDA's Office of Regulatory Affairs' (ORA's) Online Reporting Analysis Decision Support System (ORADSS), which is a data lake that contain information about companies (including the following identifiers and contact information: point of contact name, employment status, work email address, work phone number, and work mailing address) and inspections (including inspection ID, company address, inspector name, supervisor name, and lead signatory name). This information will be included in analysis to identify entities and products that are candidates for surveillance and enforcement action.

The PII data is not shared with any other system or organization.

The ODW uses FDA single sign-on (SSO) and Active Directory (AD) systems for user authentication and it does not collect or store username and/or passwords.

For additional information on non-PII data collected, please see the attached ODW PIA.

PTA -9A:	Are user credentials used to access the system?	No
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	The Opioids Data Warehouse (ODW) ingests data from: other FDA systems; other HHS components including the Substance Abuse and Mental Health Services Administration (SAMHSA), U.S. Consumer Product Safety Commission, U.S. Drug Enforcement Agency; members of the public via public media/internet/social media; and private sector sources (e.g., drug manufacturers and distributers). However, other FDA systems, federal entities, the public, and the private sector cannot access the ODW. The Opioids Data Warehouse collects disparate data to perform data analytics to: (1) better assess vulnerability points in the population; (2) anticipate changes in the crisis (identifying early trends that may be contributing to the opioid crisis); (3) target regulatory changes on an enterprise-wide level. To better evaluate social and clinical trends that are affecting the trajectory of the opioid crisis, the Center for Drug Evaluation and Research (CDER) received congressional funding to create a large-scale Opioid Data Warehouse. Users of the system include administrators (FDA Employees and FDA Direct Contractors), Developers (FDA Direct Contractors), and End-Users (FDA Employees). Access is only available within the FDA network through Single Sign On. End-Users are aligned to a specific set of data and features that are approved for their access. ODW users who access or use the system do not use personal identifiers to retrieve records held in the system.
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 Mailing Address

		Employment Status Others - Registrant ID, associate ID, and inspection ID. In support of agency health surveillance and/or enforcement actions, any type or form of PII data can be collected or ingested into the system. Names of individuals collected include point of contact name, inspector name, supervisor name, and lead signatory name. Also, company name is included. Social media data can include other forms of PII at users' discretion. Active Directory is covered in a separate Privacy Impact Assessment (PIA)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Public Citizens Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors) Other
PIA - 4:	For what primary purpose is the PII used?	While the Opioids Data Warehouse (ODW) is intended to provide an FDA enterprise-wide capability, the current version contains applications/tools that specifically addresses the following user communities: (1) The Office of Compliance (OC), (2) The Office of Communications (OCOMM), (3) The Office of Surveillance and Epidemiology (OSE), and (4) The Office of Strategic Programs (OSP). For OC, the primary purpose of the personally identifiable information (PII) used is to proactively monitor and, when necessary, quickly and precisely respond to imports, recalls, shortages, and drug supply chain issues that may negatively impact patient safety and/or are candidates for surveillance and enforcement action. For OCOMM, the primary purpose of the PII used is to enhance and automate social media analysis to understand themes, products, events, attitudes, and behaviors being discussed in online platforms. OSE and OSP PII will be included in analysis to identify entities and products that are candidates for surveillance and enforcement action.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	Provisions of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 301, including sections 353, 355, 356b, 360; and the Drug Supply Chain Security Act (DSCSA), 21 U.S.C. 581 et seq.

PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Non-Government Sources Public Media/Internet
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
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	Personal identifiable information (PII) will be shared on a need-to-know basis with Center for Drug Evaluation and Research (CDER) personnel in order to complete assigned daily tasks pertinent to opioids. FDA employees, Direct Contractors, and vendor staff with access to the system are provided notice at the time of hire that as a condition of their employment/contract with the FDA they must consent to the government's use of their PII in relation to their assigned duties. Each time personnel log on to the agency network they view and acknowledge a notice and warning of the lack of privacy while using FDA equipment and resources. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet pages. This PIA provides additional 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	Except for authentication via FDA Single-Sign On (SSO) using an FDA badge and PIV, users are

		not required to enter any personally identifiable information (PII) into the Opioids Data Warehouse (ODW) system. Submission of PII is voluntary as that term is used by the Privacy Act. However, the submission of PII is necessary for users to access and use the system. There are no methods for employees to opt out of submitting their PII and access the system. FDA employees and Direct Contractors must provide their PII for the Agency to process administrative materials and securely administer access to the ODW system. The ODW system ingests data from other systems and data sources that are outside of systems. Methods for individuals to opt-out of PII collection or use in these other systems and data sources is outside of the scope of this Privacy Impact Assessment (PIA).
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	No major changes are planned or anticipated. If FDA changes its practices with regard to the collection or handling of personally identifiable information (PII) related to the Opioids Data Warehouse (ODW), 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 e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual. In the case of PII obtained from Reddit and other social media, the ODW will be unable to contact individuals who PII is stored, processed or transmitted.
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 personally identifiable information (PII) has been inappropriately obtained, used or disclosed in any

		FDA system have several options available to resolve the situation. These individuals may contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes. Employees with such concerns can additionally work with their supervisors, the Privacy Office, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels. Contact information for these offices and resources is available across FDA's internet and intranet pages. HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all suspected breaches must be reported to the FDA Systems Management Center (SMC).
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 processes are in place, explain why not	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 personally identifiable information (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 in the course of providing the system with an authority 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. Center for Drug Evaluation and Research (CDER) performs annual reviews to evaluate user access.
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: To be able to perform their job function. For example, users will need to perform analysis to: Proactively monitor and, when necessary, quickly and precisely respond to imports, recalls, shortages, and drug supply chain issues that may negatively impact patient safety and/or are candidates for surveillance and enforcement action; Gain deeper insights into opioid supply chain patterns, trends, and variances; (3) Understand the social context surrounding drug-related themes, products, events, attitudes, and behaviors being discussed in online platforms; and (4) Understand patterns and trends in opioid dispensing/administration, abuse and diversion, distribution, and morbidity and mortality. Administrators: Administrators provide Help Desk support, which may require performing queries related to personally identifiable information (PII). Developers: To be able to complete unit testing and debugging with data similar to that which the users will use. Contractors: To be able to complete development and testing with data similar to that the users will use. These will be Direct Contractors.	
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	To obtain a privileged user account, the user applies for and obtains an Alternate Logon Token (ALT) Personal Identify Verification (PIV)

(completes and submits an e3530 form). Once the ALT PIV is granted, the user submits a request for privileged access to the Opioids Data Warehouse (ODW) System Owner for approval. The ODW System Owner (or their delegate) reviews the request and provides written approval of account creation. The ODW System Owner updates the ODW System Access Control Request Form, assigning the new user to the appropriate Role Based Access Control (RBAC) groups depending on the user's intended role within the ODW. The System Owner submits a ticket in ServiceNow to the Active Directory team to add the user to the requested ODW RBAC groups.

To obtain a system administrator accounts, the user submits a request for system administration access to the ODW System Owner for approval. The ODW System Owner (or their delegate) reviews the request, determines authorization, and provides written approval of account creation to the ODW System Administrator (or delegate).

Non-privileged users who require access to any data in ODW that might potentially contain personally identifiable information (PII) must complete an ODW account request form and submit it to their Office Coordinator. The Office Coordinator reviews and signs the completed form indicating that the new staff has a need to access the ODW and the data contained in the ODW to perform their job function. The Office Coordinator's approval confirms the individual's role and need for access. The Office Coordinator submits the form to the ODW System Owner (or their delegate). The ODW System Owner (or their delegate) reviews the request, determines authorization, and provides written approval of account creation to the ODW System Administrator (or delegate).

Accounts for ODW users who only require access to data that does not contain PII and is publicly available are automatically created when the user first logs into the system. A formal Account Request Form is not required for general user access. These users have strict limited access to only core ODW application components and only publicly available data sets that does not contain any PII. For these users, user identifying information is provided by the FDA single sign-on (SSO) and Active Directory (AD) systems each time a user enters login detail into the ODW system. This includes username, email, and organizational designation/office. This information is used to create the user account and is stored in the ODW user database. The ODW System Owner (or their delegate) and System Administrator regularly review these user accounts to update/maintain account authorization and regulatory guidelines. These accounts are subjected to all related account security controls.

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	The Opioids Data Warehouse (ODW) users are authenticated using the FDA's single sign-on (SSO) and Active Directory (AD) systems. During the authentication process, these systems communicate with the ODW, which contains (1) authenticated user information, (2) the user's associated group or office within the FDA. Within the ODW, each authenticated user is associated with levels of data access (on a per dataset/source basis). This information was developed and is maintained taking the following into account: which data each user needs to access to perform their job duties and whether the user signed the appropriate Data Use Agreements (DUAs). Through these security controls, authenticated users are limited to viewing only the data they are authorized to access.
PIA - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	All Opioids Data Warehouse (ODW) 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 Information Management and Technology (OIMT) verifies that training has been successfully completed.
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)	The retention and destruction process associated with the information contained within this system is continuously reviewed to ensure it complies

		with FDA and National Archives and Records Administration (NARA) regulations. More specifically: (1) system user access records will adhere to General Records Schedule (GRS) 3.2 Items 030 (destruction when business use ceases) and 031 (destruction 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use); (2) information technology (IT) development project records will adhere to GRS 3.1 Item 011 (destruction 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use); and (3) contract and proposal documents will adhere to GRS 1.1 Item 010 (destruction 5 years after project is terminated, but longer retention is authorized if needed for business use.); and non-substantive program subject files, including annotations, will adhere to NC 1-88-07-2 (10 years after cutoff or when no longer needed for legal, research, historical or reference purposes, whichever is the latest.).
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.