PTA / PIA: FDA - EONIMS - QTR2 - 2025 - FDA4928176

Created Date: 5/23/2025 8:35 AM Last Updated: 5/30/2025 12:38 PM

General Information

PTA / PIA Name:	FDA - EONIMS - QTR2 - 2025 - FDA4928176	**PTA / PIA ID:**	3213210
Component Name:	FDA - OC Emergency Operations Network Incident Management System	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	8
Submitter:		**Submit Date:**	5/22/2025
Next Assessment Date:	05/29/2028	**Expiration Date:**	5/29/2028
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?	Yes
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.	3/3/2023
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: Valerie Hall
PTA 01A:	POC Title and Organization	POC Title: Business Owner POC Organization: OII/OFOR/OER/DEPS
PTA 01B:	POC Email Address	valerie.hall@fda.hhs.gov
PTA 01C:	POC Phone Number	3017968249
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.	There have been no changes.

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) Office of Commissioner (OC) Emergency Operations Network (EON) Incident Management System (IMS) captures incident data regarding FDA regulated products that are, or may be responsible for causing injury, illness or adverse events. When an emergency response to an incident is required, the incident is created within EON and communications regarding the incident are managed from within the system. The EON IMS also serves as a data mart for emergency preparedness and response literature, i.e., FDA, Departmental and government emergency response plans. Through alerts/notifications to key agency officials, EON IMS is an effective knowledge management tool that provides personnel with timely awareness of public health issues involving FDA regulated products.

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.	EON IMS collects data regarding the nature of emergency incidents as reported to FDA. The GeoWeb geographical information system (GIS) portal entailed in EON IMS handles geospatial information and resources such as mapping, visualization and location data about emergency events. EON IMS handles FDA contact data (employee name, work mailing address, work phone number and work email address) as extracted from the publicly available Department of Health and Human Services employee directory website. Users access the system via single-sign-on employing multi-factor authentication. EON IMS also contains personal contact information for key FDA staff members, including home addresses, telephone numbers and email addresses. This data (home address, personal phone number, and personal email address) is needed to effectively and efficiently respond to evolving emergency situations. Submission of this data to EON IMS for emergency situations is required not specifically mandated by statute or regulation. However, it is mandatory for operational purposes in order to effectively administer the system and coordinate emergency response actions. The GeoWeb GIS element of the system will contain the name of each system user. This is required. Additionally, GIS Portal users may voluntarily add their own photographic likeness; however, submission of any information beyond name is voluntary. The FDA After-Hours Emergency Call Center element of the system may contain callers' names, phone numbers, questions about FDA-regulated products and sometimes medical symptoms. Submission of this information is voluntary. Personally Identifiable Information (PII) from FDA Employees including FDA direct contractors: Name, work phone numbers, work email address, work mailing address, photographic identifiers. PII of key FDA staff (used in emergency situation only): Home address, personal phone number, personal email address. PII from members of the public/business partners/callers: Name, phone number, medical note and symptoms. Information that may constitute PII that is volunteered by callers are medical notes. Information is stored in accordance with the National Archives and Records Administration (NARA) retention schedule.
PTA 05A:	Are user credentials used to access the system?	Yes

PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password
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 FDA Emergency Operations Network Incident Management System (EON IMS) collects, maintains and internally shares information related to emergency incidents. It captures reported incidents regarding FDA regulated products that are, or may be responsible for causing injury, illness or other adverse events. The system also collects documents (e.g., news feeds, emails, consumer complaints) and links that information to the incident. Geographical Information system (GIS) analysis is also enabled from within the system tool set. Incident data are collected so that FDA staff can manage and monitor emergencies, adverse events, product problems, recalls, and consumer complaints. These data include overall descriptions as well as many kinds of incident- or event-specific details, such as dates, pathogens, etc. These data may include physical addresses and contact information for firms and individuals (owners, veterinarians, vendor contacts, etc.) associated with the incidents. Email addresses are stored for embassy/foreign regulatory agency contacts. Email related to incidents is also stored on the system. FDA contact data is maintained primarily for communication purposes. Users access the system via a single-sign-on process that employs multi-factor authentication. Some users are Direct Contractors. GIS and location data and maps are stored in the system to help FDA staff manage and monitor incidents. These typically identify the locations of incidents or firms. Call Center information is collected for record-keeping and complaint management. This may contain callers' names, phone numbers, questions about FDA-regulated products and sometimes medical symptoms. System users do not use name or other PII to retrieve records maintained in the system.
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://eon.fda.gov/eon
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 website is to access EON IMS application. When an emergency response to an incident is required, the incident is created within EON and communications regarding the incident are managed from within the system. The EON IMS also serves as a data mart for emergency preparedness and response literature, i.e., FDA, Departmental and government emergency response plans. The following categories of individuals have access to the website: FDA Employees and Direct Contractors Users access the website via an internal intranet URL system via single-sign-on employing multi-factor authentication.
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) Biometrics/Distinguishing Features Photographic Identifiers Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Medical Notes

PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors 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 FDA uses the PII for the primary purpose of tracking callers' issues, i.e., food-borne illness outbreaks or drug recalls.
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 the Federal Food, Drug and Cosmetic Act (21 U.S.C. 301), as amended and Presidential Policy Directive #8: National Preparedness.
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 Phone 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?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The OC Emergency Operations Network Incident Management System 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.	Callers (members of the public) voluntarily submit data via phone calls. They are asked to provide PII necessary for the call data to be useful to FDA in efforts to identify and respond to public health incidents. There is no opt-out for FDA personnel. As a condition of employment, personnel consent to the agency's use of their professional contact information in relation to their work for HHS/FDA. Notification and consent as to the collection and use of contact information occurs as part of the hiring process for personnel placed in emergency response positions. HHS/FDA notify personnel of the use of their work contact information PII at the time of hire via written statements on employment forms, within orientation programs, and through the IT Security Awareness training completed prior to reporting for duty.
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.	HHS and FDA personnel are notified, and as a condition of employment consent to the use of their information by FDA and HHS at the time they are hired. To the extent system changes require notice, personnel may be notified via broadcast or individual email, internal memorandum or similar means. With regard to emergency callers, there is not a specific notification process built into FDA After-Hours Emergency Call Center system. Callers voluntarily submit data via phone calls. There is no feasible way to notify callers after the fact.
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.	FDA users may submit complaints or concerns through FDA's Employee Resource and Information Center (ERIC), to FDA's IT Security office, and to FDA's privacy office. Callers to the FDA After-Hours Emergency Call Center can raise concerns with the FDA via addresses and contact information provided on FDA.gov. In the event any employee suspects his or her information has been inappropriately accessed or used, or is incomplete, incorrect, or out-of-date, the individual can contact the Employee Resource and Information Center (ERIC), which is the employee IT help line, and request assistance. Individuals may also contact the FDA's Cybersecurity Infrastructure Operations Coordination Center (CIOCC), the Privacy Office and their supervisors and corresponding management staff. HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all reports of suspected breaches must be reported to the 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.	The process in place for periodic reviews of PII to ensure data integrity is to verify and validate all data, limit data access and permissions, perform regular access audits, and ensure that the system periodically backs up the data in its storage locations. Data availability is ensured by using role-based access control to provide users with all data necessary to perform their individual work. Data relevancy is ensured by regularly removing user information for those who no longer need access to the system. Accuracy of PII is ensured by collecting the information directly from users and having users verify that their information is correct. Due to the nature of the FDA After-Hours Emergency Call Center system, FDA relies on callers to submit accurate information themselves. Thereafter, corrections can be made as inaccuracies are identified during the course of business.
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 access PII about themselves and other users to communicate work related topics. Administrators require access to PII about users to monitor the system and manage system access. Developers require access to PII about users to add system enhancements. Contractors are Direct Contractors that are users that require access to PII to communicate on work related topics.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System users with valid network accounts who require access must acquire access by obtaining supervisor approver and signature before access is granted.

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.	Access to Personally Identifiable Information (PII) is governed by the principle of least privilege. When a user account is created, the user's supervisor specifies the minimum level of system access required for the individual to perform their job duties. This ensures that users are only granted access to the specific data necessary for their roles. Access permissions are regularly reviewed to maintain compliance with this principle. During these reviews, user access is adjusted as needed, and accounts that are no longer required are promptly removed from the system. Additionally, when a user changes positions or offices, their access is reassessed to ensure it aligns with their new responsibilities. Access is modified or revoked accordingly if the user no longer has a need-to-know or need-to-have for certain data.
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 Information Management and Technology (OIMT) verifies that individuals successfully complete the training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Users are given system-specific training related to security and privacy issues. A standard disclaimer advising users of their rights and responsibilities regarding use of a government information system appears on the online system access form for the GeoWeb GIS Portal.
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).	Retention is achieved by system backups and storage. The retention and destruction process associated with the information contained within this system is reviewed to ensure it complies with FDA and National Archives and Records Administration (NARA) regulations. Records in this system containing PII fall under NARA approved FDA Programmatic Records Control Schedule 2341a-EON IMS Data Files. The NARA citation is N1-088-09-007, Item 1.5.1.1. Data Files for Significant Emergency/Incident Management Files. This schedule directs that disposition of records is permanent. The cutoff date is at end of the fiscal year after incident investigation is completed. Transfer of records to NARA takes place 10 years after cutoff.

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 provided by the FDA Consolidated Infrastructure. Physical controls include that all of the safeguards provided to FDA servers located at FDA's WODC, to include armed 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:**	5/22/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/23/2025
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:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/27/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/27/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	4

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/30/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/30/2025 11:12 AM	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 01	BLAND, CRYSTAL	5/27/2025	5-27-2025 Per FDA's Email, The PIA is experiencing an Archer error with question General 03: Q-3 “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 3/3/2023. 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.	5-27-2025 EMAIL_PIA in Queue (OC Emergency Operations Network Incident Management System).pdf OC Emergency Operations Network Incident Management System_SOP Approved.pdf