Privacy Impact Assessment (PIA): FDA - GeoWeb - QTR2 - 2021 - FDA1950987

Date Signed: 11/12/2021

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:**	1324869
PIA Name:	FDA - GeoWeb - QTR2 - 2021 - FDA1950987	**Title:**	FDA - OC Emergency Operations Network
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	3/12/2020
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	EON IMS has implemented three minor releases since March 2020. The key enhancement, the

		added Rapid Alert System for Food and Feed (RASFF) Notices element allows Office of Emergency Operations (OEO) users to more easily capture RASFF notices sent to a particular mailbox within EON IMS. Other enhancements: a) Ability to pull edited fields from Consumer Complaint (CC) data into an "edited data fields" extract report and to pull Product Defect (PD) reports and associated edited data for PFR/LFR/CC reports into this extract. b) Additional data fields from original Consumer Complaints incorporated into the Consumer Complaint Center for Veterinary Medicine (CVM) Report tab. c) New Lab information table. d) Updated Enterprise Business Objects (EBO) with New Consumer Complaint Fields.
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 FDA 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 - 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.	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.
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	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 - 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 Photographic Identifiers Mailing Address

		Others - PII from employees including FDA direct contractor: Name, work phone numbers, work email address, work mailing address, photographic identifiers. PII of key FDA staff (used in emergency situations 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.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Public Citizens
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The primary purpose is to track callers' issues, i.e., food-borne illness outbreaks or drug recalls.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	No secondary uses for PII.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	The Federal Food, Drug and Cosmetic Act (21 U.S.C. 301), as amended and Presidential Policy Directive #8: National Preparedness.
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Other Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign Non-Government Sources Members of the Public Private Sector
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	The FDA After-Hours Emergency Call Center is a call receipt program. Callers voluntarily provide their information and are aware of the purpose for

		which they provide it to FDA. They may raise any questions or concerns about data use during their telephone discussion. Callers may also view privacy policies available on FDA.gov. 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. Each time personnel log on to the agency network they also view and acknowledge a notice and warning of the lack of privacy in the course of using FDA equipment and resources. FDA's web and privacy policies are provided on all FDA internet (FDA.Gov) and intranet pages (inside.fda.gov). 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	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 - 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	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 - 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	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 Systems Management Center (SMC), 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 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	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 - 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: FDA personnel who use the system have access to the PII for other users in order to communicate on work related topics. Administrators: Monitor the system and manage system access. Developers: Adding system enhancements. Contractors: Users are 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	Users who require access to the information system need to have supervisor approval and sign off before access is granted.
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 user's supervisor will indicate on the account creation form the minimum information system access that is required in order for the user to complete his/her job. The access list for the information system is regularly reviewed at which time users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system. The same process is followed when a user switches offices or positions the user no longer has a need-to-know or need-to-have access in order to perform authorized duties of his/her position.
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	All users complete the mandatory annual information security and privacy awareness course.

	maintained	
PIA - 21:	Describe 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 - 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 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: 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 - 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 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.