Privacy Impact Assessment (PIA): FDA - CARA - QTR2 - 2024 - FDA2128959

Created Date: 5/9/2024 8:04 AM Last Updated: 5/23/2024 4:07 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

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

PIA Name:	FDA - CARA - QTR2 - 2024 - FDA2128959	**PIA ID:**	1823363
Name of Component:	FDA - HFP CORE Analytics Research Application	**Name of ATO Boundary:**	CDRH Scientific and Research General Support Systems
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	16
Submission Status:	Submitted	**Submit Date:**	5/8/2024
Next Assessment Date:	N/A	**Expiration Date:**	5/23/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2128959
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	10/3/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	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) Center for Food Safety and Applied Nutrition (CFSAN) Coordinated Outbreak Response and Evaluation (CORE) Analytic and Research Application (CARA) system is an internal case management system used to support FDA's CFSAN CORE Network teams. CORE Network teams use CFSAN CARA to automate and streamline their business processes and enhance their reporting and research/analysis capacities to detect, respond and prevent outbreaks linked to CFSAN regulated products, and thereby protect the public health. CFSAN CARA is one of four components currently operating under the CFSAN Enterprise Information Repository for Research and Analytics boundary. FDA assesses the other components separately. The CFSAN CARA system enables users to record incident information with minimum manual data entry, delegate tasks, manage assigned incidents, investigate and analyze incidents through automated workflows, create documents and artifacts pertaining to the incident automatically with information available in the application, upload information/records (includes non-PII data only) from external sources to associate with specific incidents, communicate internally through automated notifications and collaborate with the FDA community. The system also allows FDA executive management to generate visual data reports to monitor incidents investigated by the CORE teams and for CORE Senior Leadership to monitor and manage the work progress on incidents through all stages of team engagement. CFSAN CARA is built utilizing Appian Business Process Management (BPM) suite cloud solution and is hosted on the CFSAN Appian Cloud platform. To minimize manual data entry effort/errors and promote auto-population of data collected/shared by various FDA internal and external systems, the system is undergoing integrations via the CFSAN Data Warehouse (the subject of a separate assessment). The CFSAN CARA system is used only by the CFSAN CORE Network, which is comprised of a Signals and Surveillance Team, three Response Teams, Outbreak Evaluation (OE) and Outbreak Analytics (OA) teams, and the Communication Team.
PTA - 5:	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 CFSAN CARA system collects and stores incident-specific data and business contact information. The system collects and stores personally identifiable information (PII) about FDA employees (permanent employees and Direct Contractors), Centers for Disease Control (CDC) and United States Department of Agriculture (USDA) personnel (permanent and Direct Contractors), and/or State/local government partners. PII is

		obtained from Incident Point of Contact (POC) Lists at FDA, CDC, USDA, and/or State/local government offices, as well as Incident Command System (ICS) 201 reports and email attachments. PII includes (a) name; (b) work email address; (c) business address; and (d) business telephone numbers. All PII data collected from individuals is done so in their professional capacity and is not shared with any other systems. CFSAN CARA also collects and stores the following non-PII from incident status and summary data reports: (a) incident name; (b) incident type; (c) incident description; (d) district office names; (e) CORE dates; (f) number of cases; (g) vehicle information (associated with contaminated ingredient); (h) objectives and resources for ICS 201 and 202, organizational data; and (i) incident notification source (at agency/organization level). Other non-PII collected and maintained includes: (a) product name; (b) product type; (c) product category; (d) product source; (e) firm FEI number; (f) firm name; (g) firm address; (h) firm action; (i) number of hospitalizations and deaths; (j) epidemiology data; (k) type of assignments issued; (l) action indicated; (m) 483 issuance determinations; (n) lab sample type (food and environmental); (o) lab sample dates of collection; and (p) product traced. Non-PII information is not shared with any other systems. The system does share incident level data with other applications used in various centers across the Agency to investigate, monitor, and analyze an outbreak. However, the incident level data shared with other applications does not include PII. The users of this system include system administrators (Admins-FDA employees – members of the CORE) and Developers (FDA Direct Contractors – technical support staff). Users of the system can record and store their name, work email address, business address and business phone number. Users access is based on single sign-on (SSO) authentication and personal identification verification (PIV) cards. The system providing and maintaining access credentials is Active Directory (AD). System Admins generate usernames based on existing FDA username (FDA email address). By default, user accounts contain username and name of the FDA employee. System records are retained in accordance with applicable records schedules
PTA - 5A:	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. The system providing credentials is

PTA - 5B:	Please identify the type of user credentials used to access the system.	
PTA - 6:	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 system is used to record incident specific data and CARA operations information. The primary purpose of CARA is to support CFSAN CORE Network teams including to automate and streamline their business workflow and allow users to locate incidents/outbreak information from one centralized repository. CORE captures outbreak related data (linked to CFSAN-regulated products) from other outbreak related internal FDA or external systems, and the CORE info is shared with the internal users. Therefore, the incident POC list is shared in the system. Access to CFSAN CARA requires the use of PIV card/SSO authentication. POC PII data is collected and maintained in the system to allow users to quickly reach out to incident related entity POCs to respond to reported outbreaks; the non-PII data includes all incident related attributes and are collected/maintained and shared among the CORE Network teams. User PII (name and work contact information) is required to administer access to the system and to complete processing and management of outbreak incident reports. This includes enabling follow-up communications with incident reporting entities and contacts. The operation and use of CFSAN CARA does not entail the use of PII to retrieve records stored in the system.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	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 provide users a direct way of accessing the CARA application. The following categories of individuals have access to the website: CORE Business Groups (FDA permanent employees and Direct Contractors). Users access the website via internal non-public URL.
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 - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	

PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Mailing Address User Credentials
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
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	PII is collected and stored to enable follow-up communications with incident reporting entities/POCs (from various federal, state, and local government entities) and industry to manage outbreak incidents.

PIA - 5:	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 - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The CORE system includes data and reports that support post market food safety through inspection, analyses, and control of biological, chemical, and physical hazards from production to product consumption, in accordance with 21 CFR Part 123 as authorized under provisions of Title 21 of the U.S. Code including 21 U.S.C. 321 and 350g.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Other Federal Entities Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	CARA is an internal application, so an OMB number is not generated because the paper reduction act does not apply.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	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.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	Individuals may opt-out of the collection or use of their PII by not using the system. However, submission of PII is necessary to access the system and complete assigned tasks.

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.	CORE captures outbreak related data from other outbreak related internal FDA or external systems, and the CORE info is shared with the internal users. Therefore, the incident POC list is shared in the system. In the event of major system changes, FDA will notify individuals via the most effective means such as email to users, system pop-up message, or other notice within the system. Note that for the internal FDA POCs, at the time of hire, FDA personnel and Direct Contractors are given notice on forms, web pages, and in orientation and they consent to the FDA's use of their PII in relation to their work as federal employees/ Direct Contractors. To access the system, all users must read and agree, via a mandatory pop-up box which states that by accepting they are accessing a U.S. Government system and that system usage maybe monitored, recorded and subject to the audit. 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 - 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.	Personnel may initiate corrections to PII by submitting an information update form to his or her supervisor or the FDA Badging Office. Federal employees and Direct Contractors may address their privacy concerns through supervisors, managers, and team leaders, and they may also seek assistance using FDA's Employee Resource and Information Center (ERIC), reporting potential loss or misuse of their PII to FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and/or by contacting FDA's Privacy Office directly. All system users are required to rapidly report suspected incidents and breaches.

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.	Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. User PII is relevant and necessary to be granted access to the system. PII relevancy is supported through the design of the system to require and collect only the PII elements necessary to administer the system and enable its intended use. 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 privacy and security controls selected and implemented while 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. FDA performs annual reviews to evaluate user access. If the user's name or email is incorrect, then the user would reach out to a CARA administrator. User email address is constantly validated against FDA's Active Directory (separate system). If the email address is not valid, the user will not be able to log into the CARA application.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Contractors – FDA contractors are the administrators and developers of the application, and their work necessarily requires access to the limited PII in the system. Administrators – Administrators will have access to all parts of the Appian Platform that Appian sits on including any user information. Administrators create accounts and grant access to new users and administer the database which contains user information. Developers – Developers within CARA are given administrator privileges and also have database access. Users – Users will see their own information in the application and logs of when other users modified records – for example a "Last Updated" field. They can also assign tasks to other users in the application and will see their name during the assignment.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All authorized CORE users can view the POCs associated with reported incidents. The access to the system for users and administrators/developers requires supervisor approval prior to gaining access. The business owner of CARA and administrators follow CFSAN Account Management Standard Operating Procedure (SOP) to create, deactivate, and manage the user accounts, and the user account review is conducted semi-annually to identify and remove unnecessary accounts.
PIA - 20:	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.	Technical methods applied include system-specific access settings, user authentication, and system monitoring. The access list for the information system is regularly reviewed to adjust users' access permissions and remove unnecessary accounts.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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 system users at FDA complete 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 - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	CFSAN provides users with a user security policy and associated FDA Staff Manual Guide (SMG). Personnel are trained on the use of the system and review the 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 National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	CFSAN personnel will retain records in accordance with N1-088-09-007, Item 1.5.2 Incident Outbreak Data Files Maintained in Center or Office (includes CFSAN Outbreak Surveillance Database) - Temporary. Cutoff at end of the fiscal year when the investigation is closed. Delete/destroy 30 years after cutoff, or when no longer needed for business 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.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/9/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	5/9/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/23/2024: This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	14

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Signature.docx
SAOP Comments:	Approved on behalf of Bridget Guenther	**SAOP Review Date:**	5/23/2024
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	5/23/2024 4:07 PM	**History Log:**	View History Log