Privacy Impact Assessment (PIA): FDA - FCRS - QTR2 - 2024 - FDA2129527

Created Date: 5/23/2024 12:03 PM Last Updated: 6/14/2024 4:35 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 - FCRS - QTR2 - 2024 - FDA2129527	**PIA ID:**	1833450
Name of Component:	FDA - HFP Food Code Reference System	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	24
Submission Status:	Submitted	**Submit Date:**	5/22/2024
Next Assessment Date:	N/A	**Expiration Date:**	6/14/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2129527
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.	9/9/2022
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) is responsible for promoting and protecting the public's health by ensuring that the nation's food supply is safe, sanitary, wholesome, and honestly labeled, and that cosmetic products are safe and properly labeled. CFSAN's Food Code Reference System (FCRS), a subcomponent of the CFSAN's Knowledge Management Applications system boundary, is a searchable online database that serves as a resource for federal agencies, state, local, and tribal jurisdictions, consumers, academia, and industry stakeholders involved in the prevention of food borne illnesses. Users of the system use FCRS to access Food Code interpretations (as provided by the CFSAN Retail Food Protection Team within the Office of Food Safety (OFS)) and responses to questions regarding retail food safety and the FDA standardization exercise (retail establishment inspections). CFSAN FCRS includes two user modules. Users of the internal module is limited to a very small group of FDA employees (permanent and Direct Contractors) who operate as system administrators (Admins), developers and investigators. Internal users access the system via single sign-on (SSO) authentication. Users of the external module include members of the public and non-HHS entities who are required to create a user account in order to access the system.
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.	FCRS collects and maintains the following personally identifiable information (PII) about FDA employees (permanent and Direct Contractors): job title. The FDA system providing employee data is the Enterprise Administrative Support Environment (EASE) system (the subject of a separate assessment). Employee data is used to log on authorized users automatically and securely. Non-PII collected and maintained in the system includes program related data, such as account status (active or inactive), FDA center, food code, and code provision. CFSAN FCRS also collects PII about external users of the system (members of the public; non-HHS entities; and individual users at third-party vendors). PII may include some or all of the following PII about external individuals: (a) first and last name; (b) work e-mail address; and (c) work telephone number.
PTA - 5A:	Are user credentials used to access the system?	Yes
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 FCRS is a searchable online database of FDA's interpretative positions and responses to questions related to the FDA Food Code. Designed to serve as a resource for federal agencies, state/local/tribal jurisdictions, consumers, academia, and industry stakeholders involved in the prevention of food borne illnesses, CFSAN FCRS promotes compliance with FDA food safety requirements. The FCRS application also allows OFS to assist food control jurisdictions at all levels of government by providing them with a scientifically sound technical and legal basis for regulating the retail and food service segment of the industry (restaurants and grocery stores and institutions such as nursing homes). Local, state, tribal, and federal regulators use the FDA Food Code as a model to develop or update their own food safety rules and to be consistent with national food regulatory policy. FDA employees and Direct Contractors who access or use these applications do not use any PII to retrieve records held in the FCRS application. The FCRS system is Single Sign On (SSO) and PIV enabled. The system has implemented a multifactor authentication via alternate PIV cards for network access to privileged accounts. The FDA uniquely identifies and authenticates organizational users. For PIV authenticated system, PIV credentials are based on user's certification which are also unique . The FCRS application also allows FDA CFSAN's OFS to provide a searchable database of the published Food Code. FDA uses the system to update FDA's interpretative positions and responses to questions related to the FDA Food Code. Users of the system include administrators and investigators (FDA Employees) and developers (FDA Direct Contractors). FCRS utilizes PIV cards and Single Sign On (SSO). The authenticator is managed by Active Directory and all access is managed and granted through PIV/SSO.
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)?	Yes

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 allow FDA CFSAN's OFS to provide a searchable database of the published Food Code. FDA uses the system to update FDA's interpretative positions and responses to questions related to the FDA Food Code. The FCRS system includes a website or online application that is accessible to the general public. Users access the website via 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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not Collect PII Persistent Cookies - Does Not 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 User Credentials Other - Free text Field - Job title and Center affiliation are non-PII data elements that may become PII when combined with data containing PII.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
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 PII handled in FCRS is used to manage user access and to enable contact between the FDA, federal agencies, state/local/tribal jurisdictions, consumers, academia, and industry stakeholders involved in the prevention of food borne illnesses.
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.	5 U.S.C. 301 Departmental regulations; 42 U.S.C. 243, Section 311 Public Health Service Act; Federal Information Processing Standards (FIPS) 199 and NIST SP 800-60 Rev. 1, Volumes I and II.
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.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Email Online Government Sources Other HHS OPDIV State/Local/Tribal Foreign Other Federal Entities Non-Government Sources Private Sector
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.	Not applicable. FDA is providing users with access to FDA's interpretation of the Food Code.
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.	For FCRS although the submission of all information is "voluntary" as that term is used in the context of the Privacy Act, submission of PII is necessary to coordinate and conduct oversight for the functions enabled by FCRS. There is no specific opt-out process. Individuals may decline to provide PII but will not be able to use the system.

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.	If FDA changes its practices with regard to the collection or handling of PII related to the website , 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 email to individuals, adding or updating online notices or forms, or other available means to inform the individual.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC-employees or Direct Contractors only), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel must report without delay to FDA's Cybersecurity and Infrastructure Operations and Coordination Center (CIOCC).
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	The agency reviews PII during the approval and certification process. Availability, relevancy, accuracy, and integrity of PII about FDA employees is addressed at the source system, EASE, where reviews and controls are applied pursuant to security and privacy assessments of that system as well as under organizational business practices.
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.	Users: Users require access to conduct research and perform searches. Administrators: For development, testing, and maintenance purposes. Some of the administrators are Direct Contractors. Developers: For development, testing, and maintenance purpose. Some of the developers are Direct Contractors. Contractors: Direct contractors who perform administrative, development, testing, and maintenance purpose.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users who require access to the PII in the system need to obtain supervisory approval before access is granted. There are two ways to request access to the applications: the user emails the business owner/IT Technical Lead or submits a request online through the 'Request Access' application option.
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.	Role based security controls ensure that each user role is appropriately assigned at the individual level in accordance with an individual user's need-to-know and least-access-privileges in regard to official duties such that each user sees/accesses only that data that is essential to complete his/her job. The agency reviews the access list for the information system on a quarterly basis. During this process users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
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 personnel with access to PII collected in the system are required to take mandatory FDA security and privacy awareness training annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	The FCRS application has a user manual which serves as system reference material and training.
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).	FCRS adheres to NARA approved GRS 5.2 Item 020 schedule for intermediary records-Temporary- Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. CFSAN FCRS PII records are reviewed during the periodic user access review process and retained or destroyed when no longer needed for business use.
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 on PII and implementation of Need to Know and Minimum Necessary principles when awarding access. Technical Safeguards include the use of two-factor access authentication, device disk encryption, firewalls, virtual private network (VPN) and network monitoring and intrusion detection tools. Physical controls include the location of all system servers located at FDA 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:**	5/23/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	5/23/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/29/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski 5/29/2024 Per FDA's email (see supporting documentation), they provided the correct responses to PIA-17, PIA-18, PIA-23, and PIA-24. Responses have been updated and also noted in the comment tag of each question. This PIA is now ready for SAOP review and approval. 5/28/2024 Emailed FDA Privacy in reference to their responses to PIA-17, PIA-18, PIA-23, and PIA-24. As there seem to be a sync issues of how the responses came over.	**Agency Privacy Analyst Days Open:**	6

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Please watch this PIA for stripped approvals, as the SAOP days open is inaccurate. Per FDA's email (see supporting documentation), they provided the correct responses to PIA-17, PIA-18, PIA-23, and PIA-24. Responses have been updated and also noted in the comment tag of each question. This PIA is now ready for SAOP review and approval.	**SAOP Review Date:**	6/14/2024
		SAOP Days Open:	16

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(5-28-2024) EMAIL_RE_ FDA - FCRS - QTR2 - 2024 - FDA2129527.pdf	266419	.pdf	5/29/2024 8:00 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 23	BLAND, CRYSTAL	5/28/2024	The response to PIA-23 looks likes it supposed to be part of PIA-24 response as it talks about administrative and technical safeguards. Please provide a response for PIA-23, listing a NARA approve retention schedule.	
PIA - 18	BLAND, CRYSTAL	5/28/2024	Per PIA-17, "Others" is selected but their is no response who "Others" are and why they would have access to PII in the system. Please explain who "Others" are and there reason for access to the PII in the system.	
PIA - 17	BLAND, CRYSTAL	5/28/2024	Per PIA-18, their is no response explaining who "Others" are or why they would have access to the PII in the system. If "others" isn't supposed to be selected then update accordingly.	
PIA - 23	BLAND, CRYSTAL	5/29/2024	Per FDA's Email the correct response should read as follows: FCRS adheres to NARA approved GRS 5.2 Item 020 schedule for intermediary records-Temporary-Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. CFSAN FCRS PII records are reviewed during the periodic user access review process and retained or destroyed when no longer needed for business use.	
PIA - 17	BLAND, CRYSTAL	5/29/2024	Per FDA's email, "Others" should not be selected.	
PIA - 24	BLAND, CRYSTAL	5/29/2024	Per FDA's email the correct response should read as follows: Administrative safeguards include user training on PII and implementation of Need to Know and Minimum Necessary principles when awarding access. Technical Safeguards include the use of two-factor access authentication, device disk encryption, firewalls, virtual private network (VPN) and network monitoring and intrusion detection tools. Physical controls include the location of all system servers located at FDA	

	facilities protected by guards, locked facility doors, and climate controls.

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:	6/14/2024 4:35 PM	**History Log:**	View History Log