

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 - FARM - QTR1 - 2025 - FDA4901815	PIA ID:	2804702
Name of Component:	FDA - HFP Food Applications Regulatory Management	Name of ATO Boundary:	CBER Office of Regulatory Operations
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	26
Submission Status:	Submitted	Submit Date:	3/5/2025
Next Assessment Date:	N/A	Expiration Date:	3/9/2028
Office:		OPDIV:	FDA
Security Categorization:	Moderate	OpDiv PIA ID:	FDA4901815
Legacy PIA ID:		Make PIA available to Public?:	No
1:	Identify the Enterprise Performance Lifecycle Phase of the system.		Initiation
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.		12/23/2022
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.
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?
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.
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.
PTA - 5A:	Are user credentials used to access the system?
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.
PTA - 7:	Does the system collect, maintain, use or share PII?
PTA - 7A:	Does this include Sensitive PII as defined by HHS?
PTA - 8:	Does the system include a website or online application?
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?

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.
PTA - 10:	Does the website have a posted privacy notice?
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?
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?
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?
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?
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?
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?

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 Employment Status User Credentials Other - Free text Field
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 Members of the public
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?	PII is used for communications with the FDA regarding food additive petitions and similar regulatory submissions. PII is also used to process FOIA requests.
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 Federal Food, Drug and Cosmetic Act (FDC&A, 21 U.S.C. 301) and corresponding regulations (21 CFR 71-199), the Dietary Supplement and Health Education Act (DSHEA, 21 U.S.C. Section 4), and the Food Allergen Labeling and Consumer Protection Act of 2004 (FALCPA, an element of the FDC&A, 21 U.S.C. 301), and 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission.
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 Within the OPDIV Non-Government Sources Members of the Public Private Sector

PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB Control No. 0910-0342; Expiration Date: 08/31/2025* (Pending 60-day. Sent to FDA/PRA for publishing) OMB Control No. 0910-0016; Expiration Date: 10/31/2026 OMB Control No. 0910-0583; Expiration Date: 09/30/2027 OMB Control No. 0910-0704; Expiration Date: Discontinue * (08/31/21) OMB Control No. 0910-0495; Expiration Date: 04/30/2027 OMB Control No. 0910-0330; Expiration Date: 02/28/2027 OMB Control No. 0910-0331; Expiration Date: 07/31/2025* (60-day Published 12/19/2024)
PIA - 10B:	Identify the OMB information collection approval number expiration date.	8/31/2025
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
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.	Submitters provide their contact information as a practical requirement in order to communicate with FDA and to gain access to the system. There are no opt-out procedures specific to HFP FARM. While FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity. FOIA requestors may opt not to submit a request. To submit a request and receive a response, however, requestors must provide professional PII. At the time of network logon relevant users view and acknowledge a warning message advising that they are using monitored government systems and have no reasonable expectation of privacy. The same warning is displayed to users logging into FARM via the public-facing webpage. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet pages.

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 e-mail 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.	<p>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-FDA personnel only), the Cybersecurity 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).</p> <p>HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all reports of suspected breaches must be immediately reported to the CIOCC.</p>
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. FDA personnel may correct/update their information themselves and their 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 authorization 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. HFP performs annual reviews to evaluate user access.
PIA - 17:	Identify who will have access to the PII in the system.	<p>Users</p> <p>Administrators</p> <p>Developers</p> <p>Contractors</p>
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

<p>PIA - 18:</p>	<p>Provide the reason why each of the groups identified in PIA - 17 needs access to PII.</p>	<p>Users: Receive, review and manage submissions. Some of the users are Direct Contractors.</p> <p>Administrators: Monitor the system, manage the workflow and system access.</p> <p>Developers: The FARM developers are Direct Contractors who support the development of FARM. Developers have access to the Professional PII, but no PII is collected about the Developers</p> <p>Contractors: Same as users and developers (Direct Contractors).</p>
<p>PIA - 19:</p>	<p>Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>Direct Contractors need access to the system for the purposes of user support to include error verification, validation, and smoke test procedures with regard to system updates and enhancements.</p> <p>FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.</p>
<p>PIA - 20:</p>	<p>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.</p>	<p>The relevant supervisor will indicate on the user account creation form the minimum access that is required for the user to complete his/her job. The scope of access is restricted based on role-based criteria. Technical controls and settings are applied to enforce minimum access. The access list for the information system is reviewed monthly, and users' access permissions are reviewed/adjusted.</p>
<p>PIA - 21:</p>	<p>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.</p>	<p>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).</p> <p>All personnel must complete information technology (IT) security and privacy awareness training at least once a year. Training completion is tracked by the Office of Digital Transformation (ODT).</p>
<p>PIA - 22:</p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>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.</p>

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).

HFP maintains FARM records under the following National Archives and Records Administration (NARA) General Records Schedules:

(GRS) 6.5 item 020:

Customer/client records.

Distribution lists used by an agency to deliver specific goods or services. Records include:

- contact information for customers or clients.
- subscription databases for distributing information such as publications and data sets produced by the agency.
- files and databases related to constituent and community outreach or relations.
- sign-up, request, and opt-out forms.

Temporary. Delete when superseded, obsolete, or when customer requests the agency to remove the records.

GRS 4.2 Item 20:

Files created in response to requests for information under the FOIA, consisting of the original request, a copy of the reply, and all related supporting files which may include the official file copy of the requested records or copies thereof.

HFP reviews and updates this schedule and retention and destruction processes periodically and as system changes occur.

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, 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 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:	3/5/2025
Privacy Analyst Comments:		Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP 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.	SOP Review Date:	3/5/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	3/6/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 3/6/2025 Due to sync issues when resubmitting the PIA back to OIS instance Archer this PIA has already been approved outside the tool. I have attached the Approved PIA in Supporting Documentation. 2/27/2025 This PIA is being return/rejected because the PTA is blank (of any responses). Will send Email of the external review of the PIA as we had comments.	Agency Privacy Analyst Days Open:	1

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:		SAOP Review Date:	3/10/2025
		SAOP Days Open:	4

Supporting Document(s)					
Name	Size	Type	Upload Date	Downloads	
3-04-2025 HFP Food Applications Regulatory Management_SAOP Approved.rtf	815940	.rtf	3/6/2025 9:01 AM	0	
HFP Food Applications Regulatory Management_PIM_CB.pdf	206644	.pdf	2/27/2025 10:56 AM	0	
HFP Food Applications Regulatory Management_SOP Approved.pdf	202924	.pdf	2/27/2025 9:46 AM	0	
PIA in Queue (HFP Food Applications Regulatory Management).pdf	431655	.pdf	2/27/2025 9:46 AM	0	

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	2/27/2025	<p>Archer issue impacting the PIA: The PIA is experiencing an Archer error with Question #3 of the general information. Q-3 "Does the system have or is it covered by a Security Authorization to Operate (ATO)?" The FDA instance of Archer is automatically entering the answer "No," which is incorrect. The ATO date is 12/23/2022. 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.</p>	

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

Miscellaneous Fields			
Last Updated:	3/10/2025 1:56 PM	History Log:	View History Log