PTA / PIA: FDA - DMSS - QTR2 - 2025 - FDA4919184

Created Date: 5/7/2025 4:25 PM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - DMSS - QTR2 - 2025 - FDA4919184	**PTA / PIA ID:**	3147885
Component Name:	FDA - HFP Data Management Support Services System	**ATO Boundary Name:**	HFP Knowledge Management Applications
Overall Status:	Complete	**# of Days - Open:**	54
Submitter:		**Submit Date:**	5/20/2025
Next Assessment Date:	06/23/2028	**Expiration Date:**	6/23/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	8/21/2024
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Wenmin Chen
PTA 01A:	POC Title and Organization	Project Manager, HFP/FDA
PTA 01B:	POC Email Address	wenmin.chen@fda.gov
PTA 01C:	POC Phone Number	240-402-0730
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The purpose(s) of the Data Management Support Services System (DMS3) is to improve accuracy, data entry, record management, and robust reporting processes into one functional application. A well-functioning ticketing system would enable multiple specialists with the ability to monitor the information and solutions already gathered to resolve these issues without duplicating work across applications. The current process that utilizes Jabber, SharePoint and Outlook is inefficient. The amount of dropped calls and lack of tracking or reporting causes major delays to the Food and Drug Administration (FDA)/ Food Facility Registration (FFR) mission. The relationship of this system to other FDA systems/programs/ collections is the creation of a new DMS3 will allow integration with Automated Call Distribution (ACD) so calls/emails and tickets/data will be created automatically. The creation of a single ticketing system will standardize the practice of issue reporting and resolution as well as create a central database from which solutions can be found and adapted to new issues. A well-functioning ticketing system would enable multiple specialists with the ability to monitor the information and solutions already gathered to resolve these issues without duplicating work across applications. In addition, the central database could be used to monitor issue frequency which can be used to track common or repeating issues which specialists could use to determine if these issues require a more comprehensive and consistent resolution developed. The key functional elements of the Data Management Support Services system include: Improve data entry capabilities, accuracy of data, record management, and reporting. Integrate with ACD to virtually route telephone calls and email messages to the individual agents and business areas to process. Improve operational efficacy across applications. System “users” consist of members of the DMS3 team.

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The types of information collected into the system are: Human Foods Program (HFP) DMS3 collects and stores case specific data and business contact information. This includes correspondence/inquiry and work management information including the following personally identifiable information (PII): (a) name; (b) e-mail address; (c) phone number; (d) mailing address, (e) listing of approved IP addresses (FDA licensed user), (f) food facility registration number, (g) food establishment identification number (FEI), (h) access credentials (username/ and password) for FDA licensed users, and (i) DUNS (Data Universal Numbering System). Usernames and passwords for FDA DMS3 licensed users are initially created by the system administrators. Users receive an initial welcome email where they are given a URL to setup a password within 48 hours. If a password reset is required, the user must request the administrator perform a password reset. The types of data that are maintained in and/or shared from the system is/are: By default, the user accounts contain username of the FDA employee. The PII is not shared with any other system or organization. Users access the system through single-sign-on (SSO) authentication and personal identification verification (PIV) cards. Usernames matches the user's FDA username and are standardized. These are generated by the system Admin. By default, the user accounts contain username of the FDA employee. The amount of time the PII is stored in the system is a period of five years.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username Password
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The information about DMSS business group is collected and/or maintained to record case specific data and DMSS operations information since its primary purpose is to support DMSS business group to automate and streamline their business workflow and allow users to locate information from one centralized repository. Contact information about industry users is collected and/or maintained to follow up on issues and resolutions. PII from the system/component/collection about is not shared with anyone who does not have access to DMS3 to follow up on issues and resolutions.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes

PTA 08A:	Provide the URL(s).	https://hfpinfo.my.salesforce-sites.com/Inquirypage/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The purpose of the website is to provide DMSS users a direct way of accessing the DMS3 Salesforce application. The following categories of individuals have access to the website: DMSS Business Group Users access the website via an 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 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers DUNS Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Listing of approved IP addresses (FDA licensed users)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999

PIA 25:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of collecting contact information about industry users to follow up on issues and resolutions. This is done using subject matter expert consultation responses, knowledgebase and FAQs that are delivered via email, phone, or mail.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The FDA makes no secondary use of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 USC 301, Departmental Regulations.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The PII data elements that are used to retrieve records in the system/system component/information collection are name, email address, physical address and/or phone number in professional capacity of the individual who requested services from DMSS.
PIA 29B:	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.	The System of Record Notice is currently in development.
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Phone Email
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	New system being implemented. Will work with HFP PRA team to inquire if OMB number will be required.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals voluntarily submit their information and have control over information they opt to provide in text fields. The public facing webform where individuals submit information states that email, country, and zip code are required. For other inquiry submission avenues like phone, mail and the occasional email, less information is required during the submission process. During phone inquiries, the caller's phone number is automatically collected by the system when the call is received, the internal FDA staff member will then ask the inquirer for their zip code and sometimes email address when a response cannot be given quickly on the phone and follow up is needed. Inquiries received via mail will contain a mailing address, name, and occasionally a phone number or email address. The limited inquiries received through email are typically forwarded from internal FDA employees, and will contain information like email address, name and sometimes phone number or street address. FDA website and privacy policies are provided on the page displaying the web form, and on all FDA.gov pages. Note also that an automated email is sent out to the individual containing a copy of the information they have submitted via the web form.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	When major changes occur to the system, there are process in place to **n**otify affected individuals by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the website, or e-mail notice to the individuals.
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	The processes in place to resolve an individual's concerns when they PII has been inappropriately obtained, used or disclosed include: External submitters can notify and seek assistance from FDA and HFP by phone and/or email. This information is available on FDA.gov. They may also contact the FDA Privacy Office directly via email provided on FDA.gov. FDA personnel may resolve concerns by contacting the appropriate system administrator, FDA's Employee Resource, and Information Center (ERIC) or the Systems Management Center. Personnel may correct or update their information using the appropriate Standard Form, which is the process used to make such changes used by all FDA employees, and the data would be updated in the separate human resources information system. Privacy risks are mitigated by collecting the information directly from the external user, indicating the purpose of the collection is to enable responses to their inquiry, and sharing only aggregate non-PII regarding inquiry topics.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The process in place for periodic reviews of PII to ensure the data integrity is: FDA personnel may correct/update their information themselves to ensure accuracy. Data integrity and availability are protected by security controls selected and implemented while providing the system with an authority to operate (ATO). Controls are selected based on National Institute for 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. The process in place for periodic reviews of PII to ensure data availability is: HFP performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered. The process in place for periodic reviews of PII to ensure data relevancy is: Data relevancy is maintained through web form design limiting the data submission fields to that which is necessary for system functionality and effectiveness. Accuracy of PII is ensured: Inquirer’s PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of submission with functionalities like an automated receipt email containing all information submitted on the webform.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	No

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: Only internal HFP Information Center users will have access to triage and respond to case inquiries from the public. Administrators: Administrators have access to PII to complete system and user administration as well as reporting. Some administrators are Direct Contractors. Developers: Developers have access to PII for system development purposes. Some developers are Direct Contractors. Contractors: Direct contractors will need access to facilitate system enhancements, operation and management, and reporting. Direct contractors support Administrator, developer, and project management roles.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures in place to determine which system users may access PII are: HFP establishes differing levels of permissions using in a role-based paradigm to set access limits at the individual user level. Access requests are reviewed one at a time and DMS3 System Administrators and/or privileged users update and maintain a list of active users, which includes DMSS staff, innovators, and key stakeholders. All users are granted access via Role-Based Access Controls (RBAC) and the concept of least privilege is applied. All internal FDA support staff users (FDA employees and Direct Contractors) are granted a username and password and access the site through a secure web browser. Role-based access controls are implemented to restrict access for DMS3 to authorized roles. Information flow for DMS3 data loading processes is carried out and monitored by system administrators in support of appropriate access.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	The following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: Supervisors indicate on the account creation form the minimum information system access that is required for the user to complete his/her job. The DMSS IT and business project team define roles so that each user only has the access rights necessary to perform his/her work. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system. DMS3 System Administrators and/or privileged users update and maintain a list of active users with assigned IP addresses, which includes DMSS Staff, Innovators and Key Stakeholders.

PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All users for DMS3 are required to complete the following training and awareness programs to make them aware of protecting PII: FDA's IT Security and Privacy Awareness Annual Training. HFP Privacy Team, provides privacy act guidance and training on PTA/PIA requirements as systems are implemented and reviewed. For additional privacy guidance, personnel may contact the HFP's Privacy Office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users; however, users may access general system user guidance and may arrange tailored privacy training with the Privacy Office.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Currently no records are being deleted or archived as we're working with records management to find the appropriate record schedule.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	FDA secures PII in the system using the following administrative controls: 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. FDA secures PII in the system using the following technical controls: Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. FDA secures PII in the system using the following physical controls: 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) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/20/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/30/2025
SOP Review Comments:		**# of Days - SOP Review:**	10

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 6/5/2025 All comments have been addressed. This PIA is ready for SAOP review and approval. 5/8/2025 Please review comments and update accordingly. PTA-5: Per PIA-22: include DUNS as a PII element. PTA-5B: Per PTA-5, include HHS username and password as they are stored in the system. PIA-22: Please select "User Credentials" as username and password are stored in the system and select "Other: listing of approved IP addresses (FDA licensed users)" as this can be linked to the FDA employees. PIA-28: Cite legal authority if one is not know than cite 5 USC 301, Departmental Regulations. PIA-44: Cite a NARA approve retention schedule, if one is not in place then state "Currently no records are being deleted or archived as we're working with records management to find the appropriate record schedule."	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	19

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/24/2025 2:53 PM	GUENTHER, BRIDGET	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	5/8/2025	Per FDA Email: 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.	HFP Data Management Support Services System.pdf Privacy_Assessment_HFP Data Mgmt SSS.pdf
PTA 05B	BLAND, CRYSTAL	5/8/2025	Per PTA-5, include HHS username and password as they are stored in the system.	
PTA 05	BLAND, CRYSTAL	5/8/2025	Per PIA-22: include DUNS as a PII element.	
PIA 28	BLAND, CRYSTAL	5/8/2025	For each listed SORN, please list at least one relevant Executive Order or Statute from the Authorities section. Legal authorities may be found in the system's budget documents, information collection forms, SORNs, or the program office's website. You may be able to receive help from your OpDiv's Privacy Officer, your OpDiv's Office. If no authority is known then use 5	

			USC 301, Departmental Regulations.
PIA 44	BLAND, CRYSTAL	5/8/2025	Please list the NARA's Records Control Schedules (RCS) or General Records Schedules (GRS) that apply to the record(s) that contain PII that are maintained in the system. **Common Records Follow the General Records Schedule (GRS)** System records include citations GRS. Common GRS citations are below: • General Records Schedule (GRS) GRS 3.1: General Technology Management Records. 010, Information technology development project records. Disposition Instruction: Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS2013-00050006 • GRS 3.1: General Technology Management Records. 011, System development records. Disposition Instruction: Temporary: Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required by business use. Disposition Authority: DAA-GRS2013-00050007
PIA 22	BLAND, CRYSTAL	5/8/2025	Please select "User Credentials" as username and password are stored in the system and select "Other: listing of approved IP addresses (FDA licensed users)" as this can be linked to the FDA employees.