Privacy Impact Assessment (PIA): FDA - QMIS - QTR3 - 2024 - FDA3614359

Created Date: 8/19/2024 4:03 PM Last Updated: 8/28/2024 2:13 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 - QMIS - QTR3 - 2024 - FDA3614359	**PIA ID:**	2131575
Name of Component:	FDA - OII Quality Management Information System	**Name of ATO Boundary:**	ORA Quality Management Information System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	9
Submission Status:	Submitted	**Submit Date:**	8/19/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA3614359
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?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	10/13/2023
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to this system since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved
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.	Food and Drug Administration (FDA) Quality Management information System (QMIS) allows Office of Regulatory Affairs (ORA) components in the headquarters' offices, districts, and laboratories to standardize and automate quality management related business practices. The system allows end users (agency personnel, direct contractors (badged FDA credential holders) and external contractors) to automate document control, automate management review, and initiate corrective/preventive action. QMIS serves as a catalyst to harmonize quality management practices agency wide and reduce lifecycle costs. Additionally, QMIS ensures that FDA decision-based processes are transparent, traceable, and reportable as mandated by ORA.

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 type of information contained in QMIS consists of: internal standard operating procedures (SOPs); policies and other directives governing ways the agency does business; documents and maintenance data for active document lists; master lists; reports; correspondence such as agency-wide announcements and memoranda; quality control records related to internal work products; internal audit reports; management reviews; corrective and preventive action documentation; and, complaints and feedback related to the quality of work products, processes and services provided by the FDA. QMIS collects the first and last name, user identification number, and work e-mail addresses of the system users. Only FDA email addresses are used in the system. No personal email addresses are collected. Only authorized personnel have access to user information. Users have access to the system after logging on to the agency network via the single-sign-on (SSO) process using multi-factor authentication. There is no system-specific user name, password or other access credential information used or maintained in QMIS.
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.	HHS User Credentials HHS Username
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.	QMIS collects document control change requests, corrective actions, preventive actions, work-related feedback and complaints, audit reports, management reviews, and record control information. Complaints entered in QMIS are strictly related to the quality issues of ORA/FDA work products and processes, and do not include complaints regarding personnel issues. QMIS collects the following PII information: First and Last name, user identification number, and FDA work e-mail addresses of the system users. The data in QMIS is not shared with or accessible through any other system. ORA does not use name or other PII to retrieve records held 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?	No
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?	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 Other - Free text Field - User Identification No.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ 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 personally identifiable information (PII) is collected to create user accounts and task notifications. Tasks include the work which may be assigned to employees for completing a review of a document, completing a form in the system, or completing training.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None.
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
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 Email Government Sources Within the OPDIV 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.	System is not subject to the PRA.
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.	Users cannot opt out of the collection or use of their PII. It is required to establish user accounts and to authenticate system access. Users who do not have an account in QMIS can access stored documents using a guest access process without providing PII. Guest access requires supervisor (Administrator) approval. Guest access does not require PII and limits the user's access to a read-only view of documents, based on a need to know, that do not contain PII, and are in a protected PDF format.
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.	The Quality Management Systems (QMS) office communicates with users through regularly provided e-mails, online notices and forms, and/or newsletters. If there is any change to the system, or if the use or collection of user PII changes, users will be notified of that change through those avenues. However, no such changes are anticipated.
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 several methods of recourse available. These individuals may contact FDA offices via email, phone and standard mail avenues (all listed on fda.gov and the agency's intranet). Offices available to assist include FDA's Employee Resource Information Center (ERIC Helpdesk), the FDA Systems Management Center, and FDA's Privacy Office. HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all reports of suspected breaches must be reported to the SMC.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	Users provide PII voluntarily. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. 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 NIST guidance. ORA performs annual reviews to evaluate user access. Data discrepancies identified during system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators 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 access PII about themselves and other users to: Users can only access their own PII. While external contractors are users of QMIS, they do not have access to the PII data in their role as users. Administrators require access to PII about users to: Administrators (including the help desk/apps desk) create user accounts using the supplied PII and review user access rights. While they may perform the role of an administrator of QMIS, external contractors do not have access to the PII data as administrators of the system. Direct Contractors access accounts/PII to troubleshoot issues with the system. Direct contractors have access to System Administration roles as described in the Design Maintenance Enhancement (DME) contract. External contractors do not have access to the PII data in QMIS.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users can only access their own PII. While external contractors are users of QMIS, they do not have access to the PII data in their role as users. Administrators (including the help desk/apps desk) create user accounts using the supplied PII and review user access rights. While they may perform the role of an administrator of QMIS, external contractors do not have access to the PII data as administrators of the system. Direct Contractors access accounts/PII to troubleshoot issues with the system. Direct contractors have access to System Administration roles as described in the Design Maintenance Enhancement (DME) contract. External contractors do not have access to the PII data in QMIS.
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.	General users of the QMIS can only access their own PII while Administrators and Developers have access to PII in the amount necessary to perform their job duties. All QMIS users are provided Role Based Access control (RBAC) with least privilege (only the necessary rights to perform their job functions) access. New QMIS users are required to have their supervisor create a help desk ticket which then is required to be approved by a Quality Service Manager (QSM). The user's supervisor works with the QSM to ensure the level of access needed for the user.
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 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).

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Access to QMIS is granted only after an individual has completed system training. QMIS use training and guidance materials that are available on the QMIS intranet page. Individuals may also request additional training by contacting the QMIS help desk.
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).	Electronic Records Retention-FDA Programmatic Records Control Schedules: 8420 (NARA No. NC 1-88-07-2; Program Management files), 8123 (NARA No. N1-088-06-3; Administrative Correspondence), and 4913 (NARA No. N1-088-08-3; Employee Training Records). Records are temporary per the above retention schedules, as follows: 8420 Program Management files: Cutoff after the final action/report or at end of the calendar year. Maintain a minimum of 3 years then destroy 7 years after cutoff or when no longer needed for reference, whichever is sooner. 8123 Administrative Correspondence: Cut off at end of each calendar year. Destroy or delete 2 years after cutoff. 4913 Employee Training Records: Cutoff at end of the fiscal year after employee leaves the Department. Delete/destroy 5 years after cutoff.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	There are several controls in place for the securing of PII within QMIS. The administrative controls include system users completing an access request form and a access review/approval process. The technical controls include firewalls, virtual private networks (VPNs), encryption, and intrusion detection systems. The physical controls are comprised of guarded facilities, gated access to these facilities, security barriers, and locked doors.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	8/19/2024
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:**	8/19/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/21/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/21/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	8/28/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 10C	VILLAFUERTE, NESTOR	8/20/2024	Please write out acronym "PRA".	
PIA - 16	VILLAFUERTE, NESTOR	8/20/2024	Please write out acronym "NIST".	
PIA - 15	VILLAFUERTE, NESTOR	8/20/2024	Please remove the period at the start of the response.	

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:	8/28/2024 2:13 PM	**History Log:**	View History Log