PTA / PIA: FDA - CBER QMIS - QTR4 - 2025 - FDA5027489

Created Date: 11/5/2025 3:25 PM Last Updated: 12/10/2025 11:24 AM

General Information

PTA / PIA Name:	FDA - CBER QMIS - QTR4 - 2025 - FDA5027489	**PTA / PIA ID:**	3971255
Component Name:	FDA - CBER Quality Management Information System	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	34
Submitter:		**Submit Date:**	11/5/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	FDA
Security Categorization:	High		
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.	12/31/2025
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	Christopher Kiem
PTA 01A:	POC Title and Organization	System Owner
PTA 01B:	POC Email Address	Christopher.Kiem@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-8093
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.	Center for Biologics Evaluation and Research (CBER) Office of Regulatory Operations (ORO) supports CBER's mission to protect and enhance the public health through the regulation of biological and related products including blood, vaccines, allergenics, tissues, and cellular and gene therapies. CBER ORO also tracks Post Marketing Commitments related to these approved products and is used for the tracking and evaluation of post market safety surveillance activities. The CBER Quality Management Information System (QMIS), which is a component of CBER ORO system supports laboratory accreditation by defining, tracking, understanding, and continually improving processes and methods. CBER QMIS serves as a document control and management system for core CBER processes, including document control, management, corrective actions, complaints, and record control. The system is housed in the FDA's Ashburn Data Center (ADC) in Ashburn, VA 20147, which Peraton operates for the FDA. CBER QMIS employees and contract staff administer the application, while Peraton provides data center and infrastructure support as well as information technology hosting services for FDA applications and components. The ADC operates as a "lights out" facility, meaning all administration, maintenance, and operational management is conducted remotely, with only facility personnel maintaining a continuous physical presence at the location.
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 type of information contained in CBER QMIS consists of: Standard Operating Procedures (SOPs); policies and other directives governing how the agency conducts 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. CBER QMIS maintains the following PII: (a) Name, (b) user identification number; and (c) 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. CBER QMIS user community includes FDA Employees and Direct Contractors. The system utilizes FDA's authentication credentials along with the user's Personal Identification Verification (PIV) card to log into the system via FDA Single Sign-On system (SSO).

PTA 05A:	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.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory
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.	CBER QMIS is a web-based software program that automates quality management processes. CBER staff use the software program for managing local quality processes and automating notification routes through Microsoft Outlook. CBER QMIS provides end users with one source that is pre-configured and provides easy access to all standard operating procedures (SOPs), forms, and other quality documents and records at the local level and throughout CBER. The quality control process includes document control, complaint/corrective/preventive action (CAPA) management, internal audits, management review, improvements, and quality records management. CBER 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 CBER QMIS are strictly related to the quality issues of CBER/FDA work products and processes, and do not include complaints regarding personnel issues. The data in CBER QMIS is not shared with or accessible through any other system. The system maintains minimal PII, limited to employee names, user identification numbers and work email addresses (FDA addresses only - no personal emails collected). CBER personnel who access or use the system do not use any personal identifiers to retrieve records held in the system.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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.	Biographical Information Name Contact Information Email Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	User identification number
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
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 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 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.	Collecting this information is necessary to meet the FDA's requirements for conducting submission review and surveillance under the provisions of the Federal Food, Drug, and Cosmetic Act at 21 U.S.C. 301, see especially sections 505A, 506B, and 522. Additional information concerning these activities may be found in CBER’s regulations at 21 CFR 600.80; 5 U.S.C. 301.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Online
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.	This component does not collect information using an information collection request as defined by the Paperwork Reduction Act.
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.	FDA notify the system users (agency personnel and direct contractors) of the agency's collection, creation and use of their PII at the time of hire (forms, webpages, new employee orientation sessions). Users voluntarily self-request access to CBER QMIS through the FDA Intranet or FDA Help Desk. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet (https://www.fda.gov/about-fda/about-website/website-policies) pages. This Privacy Impact Assessment (PIA) provides further notice.
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.	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 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.	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), 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 immediately report this information without delay to the FDA's CIOCC. In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's CIOCC.

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.	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 in the course of providing the system with an authority to operate (ATO). Controls are selected based on 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. CBER performs annual reviews to evaluate user access.
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?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: Users have access to PII in the course of reviewing applications for regulatory and scientific merit. Administrators: Administrators ensure the proper controls are in place for user access, but administrators do not review industry-submitted content or FDA analysis of that content. Developers: Developers build new capabilities for reviewers to use, but they do not review industry-submitted content or FDA analysis of that content. Contractors: Direct Contractors are sometimes developers and have access only to such material as developers have. Direct Contractors provide the technical support for the development, maintenance and issue troubleshooting for the system.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	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.

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 relevant supervisor will indicate on the user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria.
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 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). The FDA Office of Digital Transformation (ODT) verifies that individuals successfully complete the training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.
PIA 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).	Retention and destruction of PII conform to the following: GRS 5.1 Item 020 Non-recordkeeping copies of electronic records. Disposition: Temporary. Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use. GRS 5.2, Item 010 Transitory records. Disposition Temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule.
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.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	11/5/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	11/5/2025
SOP Review 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.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/26/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/26/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	21

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	12/9/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	13

SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/9/2025 2:12 PM	BAUR, VANESSA	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
No Records Found				