PTA / PIA: FDA - DPAMC - QTR2 - 2025 - FDA4943204

Created Date: 6/24/2025 12:45 PM Last Updated: 6/25/2025 8:45 AM

General Information

PTA / PIA Name:	FDA - DPAMC - QTR2 - 2025 - FDA4943204	**PTA / PIA ID:**	3393570
Component Name:	FDA - CDER DPA MasterControl	**ATO Boundary Name:**	CDER St. Louis Laboratory Informatics System
Overall Status:	Complete	**# of Days - Open:**	1
Submitter:		**Submit Date:**	6/24/2025
Next Assessment Date:	06/24/2028	**Expiration Date:**	6/24/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**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?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	4/23/2024
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	Sara Grabowski
PTA 01A:	POC Title and Organization	POC Title: Quality Assurance Specialist POC Organization: OPQ/OQA/QAS
PTA 01B:	POC Email Address	sara.grabowski@fda.hhs.gov
PTA 01C:	POC Phone Number	314-539-7541
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 Office of Pharmaceutical Quality Research (OPQR) Master Control (MC) is an electronic tool and repository that manages components of the quality management system (QMS). Information collected is to create individual user accounts. Division of Pharmaceutical Analysis (DPA) Quality Management Information System (QMiS) software supports the DPA Quality Management System (QMS) System (also known as DPA MasterControl), in defining, tracking, understanding, and continually improving processes and methods. QMiS is a web-enabled database system by the company Master Control, serving all of DPA to document and control core laboratory processes, including work instructions, training management, instrumentation, maintenance records, corrective actions, complaints, and document control. This system allows input, storage and reviewing information regarding laboratory accreditation, defining, tracking, version control, and continually improving processes and methods.
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.	United States (U.S.) Food and Drug Administration's (FDA) Center for Drug Evaluation and Research (CDER) Division of Pharmaceutical Analysis (DPA) Master Control (MC) System will collect information on employee status, position descriptions, approved policies, procedures, employee training requirements and records, request, and approval of changes within DPA MC. Information collected will also include internal quality audit information, attendance records for training or classes, instrumentation records, qualification, and supplier contact information. PII collected includes FDA employee and Direct Contractor name, email address (business), education records (is not stored or viewed by anyone with access to DPA MC, it is listed on the default display), user credentials, electronic signature, user training records, and analyst unique ID number. PII that is accessed on material and service providers (suppliers) including repair and maintenance technicians is contact name and access credentials (This information is collected to identify suppliers and if they are acceptable to use (verify they have/provide customer support information, shipping paperwork, product name/ unique ID (like a lot number), and product documents. Technician names are not entered in DPA. That information is stored in QMIS, only information entered is the level of access credentials the vendor provides a technician. Suppliers are evaluated by DPA MC for their ability to provide laboratory materials or services that are of acceptable quality for use in the laboratory. Equipment supplier information such as company, address, phone, e-mail address, supplier’s contact name, service technician or sales representative is

		stored within QMiS. Suppliers' information that is considered PII includes supplier's point of contact name, work mailing address, work phone, and work e-mail address. This information is stored within QMIS and can be viewed in DPA MC. The information collected into the system is for internal use to create individual user accounts for the system. The types of data that is maintained in and/or shared from the system is mostly records related to QMS components. Employees access DPA MC through enterprise SSO (Single Sign-On) authentication using a Personal Identity Verification (PIV) card. The system may also be accessed using username and password. User accounts are deactivated when no longer with the agency. Data will be stored in the system in accordance with the National Archives and Records Administration (NARA) records retentions standards.
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 Non-HHS User Credentials 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.	QMiS collects and stores information regarding laboratory accreditation, laboratory testing results, employee training records, version control, and improvements to DPA MC processes and methods. QMiS eliminates the need for paper records on these topics. The system is used to share approved documentation with DPA MC users and replace the use of shared computer drives or paper documentation for document management. Tracked activities and objects include the following: Job training requirement information for users. User training including name, training assignments, and date/time of completion. Date/time of renewal/update training, where applicable. Work instructions for laboratory processes including instrument use, methods, and standard operating procedures. Management of changes to documents describing standard operating procedures. Change requests and justifications for equipment configurations, methods, procedures, or processes. Laboratory non-conformances and actions that were taken (name, date, description, and action). Instrumentation records including identification, location, qualification, maintenance, repair and status. Internal audit findings and actions. Supplier and vendor name and contact information. PII is collected because the system requires name to create username, email to send notifications, supervisor to notify when tasks are overdue.
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://qmis-cderstl.fda.gov/mc/login
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 store records for the Quality Management system (QMS). The following categories of individuals have access to the website all OPQR and designated Office of Quality Assurance (OQA) staff. OPQR and OQA Staff are HHS Employees and Direct Contractors. Users access the website via login through an HHS internal online portal. Employees access DPA through enterprise SSO (Single Sign-On) authentication using a Personal Identity Verification (PIV) card. The system may also be accessed using username and password.
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.	Biographical Information Name User Credentials Education Records Employment Status/History 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.	Electronic Signature User Training Records Analyst unique ID (Identification) number Material and service providers (Suppliers) contact name and access credentials including repair and maintenance technicians are accessed in DPA MC but are stored in QMIS.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499

PIA 25:	For what primary purpose is the PII used?	The primary purpose for FDA's use of PII is to create user accounts in the system to allow staff access to perform tasks as needed.
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.	The implementation of this system is authorized by 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. In addition, the security and privacy measures of the system are required by the Federal Information Security Modernization Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
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 username (first/last name).
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.	OPM/GOVT-1 General Personnel Records SORN 09-90-0018, Personnel Records in Operating Offices, HHS/OS/ASPER.
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV
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.	The system holds no information collected under the Paperwork Reduction Act. The information is only used to create accounts in the system and process tasks.
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.	Submission of PII is voluntary as that term is used by the Privacy Act. However, the submission of PII is necessary because FDA must use this information to comply with internal FDA policies and International Standards Organization (ISO) accreditation policies. The FDA Staff Manual Guide SMG 2020 (FDA Quality System Framework for Internal Activities) defines the Quality System framework required for FDA regulatory activity, and FDA laboratories are required to comply with the ISO 9001 and 17025 standards.
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.	The PII use statement is reviewed with employees when they receive access to the QMIS system as part of New Hire Orientation. New Hire Orientation and the QMIS User Change Request form are controlled documents that cannot be modified without approval. In addition, the QMIS software is validated for use at DPA MC. No changes can be made to function or content without approval through our Change Management Procedures. The Change Request includes an evaluation of the impact the requested change will have on the QMIS system. In the event a change to the QMIS system is needed as a result of a change, an evaluation of the impact to the validated software and users is completed. Actions that impact users (i.e. change in PII collected), must be approved by Management and Quality, forms and notification information to the users updated and notification of the change is distributed to all users impacted 30 days prior to the implementation of the change. If FDA changes its collection or handling of PII in DPA Master Control 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 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 several avenues available to seek assistance. Employees may contact their supervisors, the FDA Privacy Office or seek assistance via FDA's Employee Resource Information Center (ERIC). All reports of unauthorized access, use or disclosure of PII will be reviewed and processed per FDA and HHS guidelines and federal requirements. Under federal, HHS and FDA policy, all permanent employees, Direct Contractors, and other individuals performing services for or on behalf of FDA must immediately report all known or suspected incidents and data breaches to the Cybersecurity Infrastructure Operations Coordination Center (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.	The PII information collected, accessed and used at DPA MC is controlled by our approved procedures. QMIS is the software tool used to collect and access the PII needed for compliance at DPA MC. These approved procedures are revision controlled, reviewed, and approved as part of our Quality Management System. DPA MC procedures are subjected to mandatory periodic reviews for lab compliance every three years. This periodic review process is in place to ensure documentation at DPA MC is kept accurate and relevant to our processes and mission at DPA MC. This includes any PII collected, accessed and used at DPA MC for compliance to these procedures. In addition, a description of the availability of PII and the integrity of the QMIS system in handling PII used at DPA MC is included in our procedure on Signature Integrity, Accountability and Traceability and in our procedure on Data Integrity at DPA MC. These procedures require periodic review and retraining by all current QMIS and Data Collection Software users at a minimum of every three years. These procedures are also part of our New Hire Training Program for all new users. Reporter'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 reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. 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 security controls selected and implemented in the course of 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. CDER 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 in the course of system use are addressed when discovered.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators 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.	System users' and administrators' access is controlled by QMiS's role-based access controls, depending on their designated user groups and administrator groups. Users cannot see other user records, supervisors can only see their direct reports' PII, and administrators may has access all PII for the limited purposes of administering the software and creating necessary reports when requested. Contractors: HHS Direct Contractors are system users and administrators.
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 governed by the Role Based Access Control (RBAC) policy. Access is role based, and system users access the minimum amount of information necessary to perform their job.
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.	There are three levels of access in QMIS. Quality assurance is the system administrator for the QMIS system and that function has access to all information in QMIS to run reports, set up reports, manage users and make changes that have been requested and approved. This role is independent of lab personnel and has no direct authority of their positions. The functionality of the system has been validated with limited user access based on the following (2) additional respective roles in QMIS. Change to roles or rights would require approval by Management and Quality Assurance. Current roles include a general user or trainee with access to view their own training information and history and the required training for all tasks at DPA MC. Lab Chief or Supervisor role which has access to training for only their direct reports as needed to manage the lab function.
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 Information Management and Technology (OIMT) verifies that training has been successfully completed and maintains a record of certificates of training on all FDA employees and Direct Contractors.
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 are provided privacy guidance on the FDA intranet and from Privacy staff.

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).	Information will be stored in the database for the retention period for "Personnel Records" according to 36 CFR (Code of Federal Regulations), Chapter XII, Subchapter B- Records Management. Archived records are accessible to Administrator only. Electronic Records Retention-FDA Programmatic Records Control Schedules: 8420 (NARA No. NC 1-88-07-2, Item 3.2; Program Management files), 8123 (NARA No. N1-088-06-3, Item 1.2.3; Administrative Correspondence), and 4913 (NARA No. N1-088-08-3, Item 1.1.3; 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 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 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:**	6/24/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/24/2025
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:**	6/25/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/25/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/25/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/25/2025 7:45 AM	BLAND, CRYSTAL	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	6/24/2025	Attached exported PIA.	CDER DPA MasterControl_SOP Approved.pdf