PTA / PIA: FDA - DMQS Intune - QTR4 - 2025 - FDA5066880

Created Date: 11/20/2025 3:32 PM Last Updated: 12/10/2025 11:24 AM

General Information

PTA / PIA Name:	FDA - DMQS Intune - QTR4 - 2025 - FDA5066880	**PTA / PIA ID:**	4000177
Component Name:	FDA - CDRH Division of Mammography Quality Standards Microsoft Intune	**ATO Boundary Name:**	CDRH Reporting and Collection Tools
Overall Status:	Complete	**# of Days - Open:**	21
Submitter:		**Submit Date:**	11/28/2025
Next Assessment Date:	12/08/2028	**Expiration Date:**	12/8/2028
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.	Initiation
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?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Wesley Friend
PTA 01A:	POC Title and Organization	IT Specialist Division of Mammography Quality Standards
PTA 01B:	POC Email Address	wesley.friend@fda.hhs.gov
PTA 01C:	POC Phone Number	(301) 796-5923
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	The Center for Devices and Radiological Health (CDRH), Division of Mammography Quality

those functions in support of HHS.

Standards Intune (DMQS Intune), is an instance of Microsoft Intune Federal Risk and Authorization Management Program (FedRAMP) Authorized cloud service that enables CDRH DMQS to manage and support Food and Drug Administration (FDA)-issued laptops used by state government employees who conduct inspections of nearly 8,000 Mammography Facilities in the United States. These state inspectors do not have access to the FDA Network or Active Directory and instead rely on the Facility Inspection Support Subsystem (FISS) software developed in-house by DMQS to facilitate inspections at facilities, ensuring that sensitive data is protected and compliant with regulatory requirements. DMQS Intune is used to manage and facilitate patch management, software updates, and remote support for the FDA-issued laptops. Additionally, CDRH DMQS uses Microsoft Autopilot to preconfigure devices before shipping them to inspectors, ensuring that all necessary settings and configurations are in place. The system also enables DMQS to monitor policy compliance and push software updates to inspector laptops, including the FISS application. DMQS Intune is used by CDRH DMQS Administrators, who are responsible for managing and supporting the laptops used by state inspectors. State inspectors themselves do not directly access the DMQS Intune.

CDRH Division of Mammography Quality Standards Intune (DMQS Intune) is a public-facing Software as a Service (SaaS) instance of Microsoft Azure Intune, a FedRAMP authorized cloud service. The primary purpose of DMQS Intune is to enable the CDRH DMQS to administer, patch, and update software on Mammography Quality Standards Act (MQSA) laptop computers used by inspectors to conduct inspections under the MQSA. By leveraging DMQS Intune, CDRH DMQS can ensure that MQSA laptop computers are secure, up-to-date, and compliant with regulatory requirements.

DMQS Intune provides a range of functionalities to support the CDRH DMQS's mission. These include: (1) ease of deployment, allowing for quick and efficient setup of MQSA laptop computers; (2) automatic connection to patch servers, enabling laptops to begin scanning and receiving updates as soon as they connect to the internet; (3) push software updates, including the application used by inspectors; (4) remote support capabilities, allowing administrators to troubleshoot and resolve issues with inspector laptops; and (5) policy compliance monitoring, ensuring that MQSA laptop computers remain compliant with regulatory requirements. By leveraging these functionalities, the CDRH DMQS can ensure that MQSA laptop computers are secure, reliable, and compliant with regulatory requirements.

There are three types of users within the DMQS Intune: users, administrators, and inspectors. Users are FDA employees who have been assigned MQSA Inspection Laptops for the purpose of

		conducting inspections. Administrators are FDA-DMQS System Administrators who are responsible for administering Microsoft Intune and the MQSA Inspection Laptop. Inspectors are state government employees who conduct inspections on behalf of DMQS under a contract with FDA. All users will have a username, password, and email address created in Microsoft Intune, and will use multi-factor authentication to access the system. The system will maintain minimal user information, and users will not have access to the FDA Network or the FDA Active Directory. Inspectors will use MQSA laptop computers to conduct inspections, and do not have access to FDA IT Resources.
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 First Name, Last Name, usernames, email addresses, Internet Protocol (IP) address, Media Access Control (MAC) addresses and events/activities. The information is for the creation of user accounts on the system. Device identification information (Serial numbers, device IDs for the managed laptops), User role/assignment data (To distinguish between administrators, users, and inspectors), and Authentication logs (For multi-factor authentication and access monitoring) are also collected for tracking purposes. The PII is stored in accordance with the National Archives and Records Administration (NARA) records retention schedule.
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 Email Address HHS Username Password Non-HHS User Credentials Username Password Email Address
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.	System Administrators username, email address, first and last name, IP address, events/activities are recorded for the purposes of creating their accounts and for tracking events/activity on the system. End Users username, email address, first and last name, IP address, mac address, events/activities are recorded for the purposes of creating their accounts and authenticating users. This will enable us to log events and track who performed a particular action.

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://login.microsoftonline.com/
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 this site is for the administration of laptop configuration and policies of the MQSA Laptop Computers used to conduct MQSA Inspections. Intune will provide the interface used to administer Microsoft 365 Intune Tennant. The site will only be accessed by authorized administrators. The uniform resource locator (url) is public facing but requires a system administrator account, password and Multi-Factor Authentication (MFA)/Single Sign-On (SSO) to access. System administrator will access the system using SSO.
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?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
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?	Yes
PTA 21A:	What are the AI tools and how are they used?	Microsoft Intune Copilot is an artificial intelligence (AI) assistant built into the Intune Admin Center that helps IT admins manage devices, policies, and apps using natural language. It's part of Microsoft Security Copilot; it leverages generative AI to analyze Intune data and recommend actions. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

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 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.	Internet Protocol (IP) address and MAC addresses
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/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 that PII is used is for creating user accounts and for tracking events/activity on the system. The PII used will enable CDRH to log events and track who performed a particular action.
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 Medical Device Amendments to the Food Drug and Cosmetic Act, including the Medical Device Amendments 21 U.S.C. sections 360, 360c, 360e, 360i, 360j, 360l, 510(k), 515(c), 515(d), 515(f), 519, 520(g), 520(m), and 564. Mammography Quality Standards Act Regulations (MQSA), 42 U.S.C. 263b. Safe Medical Device Act of 1990 (SMDA), 21 U.S.C. 301, 42U.S.C. 263b-n. Medical Device Reporting regulations at 21 CFR 803, 803.32, and 803.40; 21 U.S.C. 352, 360, 360i, 360j, 371, 174. The Radiological Health regulations CFR 1002.1(c)(4), 1002.10-1002.13, 1002.20, 1020.30(d), and 1020.30(d)(1), as well as Table 1 in 21 CFR 1002.1(b); 21 U.S.C. 352, 360, 360i, 360j, 360hh-ss, 371, 174. The Federal Food, Drug, and Cosmetic Act, section 519(f).
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 Email Government Sources State/Local/Tribal
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.	CDRH Division of Mammography Quality Standards Microsoft Intune does not fall under the definition of "information collection request" in the Paperwork Reduction Act (PRA).
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Private Sector
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	FDA shares first name, last name and email address with Microsoft for the purpose of creating accounts.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	None
PIA 32D:	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.	The logging/tracking/account is done in server log files.
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.	The system contains PII relevant to users' access credentials. There is no method for individuals requesting application access to opt not to submit PII. Permanent employees, Direct Contractors, and other personnel must provide their PII in order for the Agency to process administrative materials and securely administer access to component.
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.	No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the web site, or email 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.	Individuals internal to FDA can contact the FDA Privacy Office or their branch chief. Individuals' external to FDA can contact MPRIS Computer Support cdrhmqrp@fda.hhs.gov.
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 system log files are reviewed on a monthly basis to verify the integrity, availability and relevancy of data and that the accuracy of PII is insured. All users of this application, are responsible for providing accurate information and may independently update and correct their information at any time. All information is relevant to the authentication and authorization process. Integrity and availability are protected by security safeguards selected based on guidance from the National Institute of Standards and Technology (NIST) appropriate to the level of risk associated with the application.

PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors Others
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 38C:	Identify the additional person(s) who will have access to the PII in the system not mentioned in the list above.	FDA Division of Mammography Standards Information Management Team
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: (FDA employees/Direct Contractors) who have been assigned MQSA laptops for the purpose of conducting inspections. Administrators: (FDA employees) require access to PII about users to create end user, administrator and device accounts. Contractors: Direct Contractors are also inspectors.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrator accounts are only created at the direction of Division Management or Team Leads.
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.	Microsoft 365 uses a layered security approach to ensure users accessing PII only see what's necessary. Key methods included Role-Based Access Control (RBAC) to limit permissions, Conditional Access to enforce identity and device checks, and app protection policies to safeguard data within apps. Compliance profiles ensure devices meet security standards, while Just-In-Time and Just-Enough-Access minimize exposure by granting temporary, scoped access. These controls align with Zero Trust principles to verify identify, enforce least privilege, and assume breach.
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 systems users at FDA take annual mandatory cybersecurity 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 (to include any special restriction on data use and/or disclosure). The FDA Office of Digital Transformation (ODT) verifies and documents that training has been successfully completed.
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 also complete Significant Security Responsibilities Role-Based Training and Information System Contingency Planning Training. On-the-job or informal training may be received, and privacy guidance is available 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).	The following process and guidelines are in place for the retention and destruction of PII: The Microsoft Intune project records will be managed on SharePoint until they are eligible for destruction in accordance with the following NARA-approved records schedules: FDA-9911, General Records Schedule (GRS) 3.1, Item 040 – Oversight and Compliance: Destroy 5 years after the project/activity/transaction is completed or superseded. FDA-9931, GRS 3.1, Item 020 - General Technology Management records: Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. FDA-9951, GRS 3.2, Item 010 – Information System Security Records: Destroy 1 year after the system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. FDA-9991a2, GRS 3.1, Item 011 – System Development Records: Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes
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.	PII is safeguarded through a layered approach combining administrative, technical and physical controls. Administrative controls include the enforcement of privacy policies, role-based access and staff training to ensure responsible data handling. Technical safeguards include PII is protected with encryption, access controls, and monitoring to detect and prevent unauthorized use. Physical controls include secure facilities and device management practices prevent unauthorized access to systems and data. 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. Together, these controls ensure comprehensive protection of sensitive information.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	11/28/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	11/28/2025
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:**	12/1/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/1/2025 All comment addressed. This PIA is ready for SAOP review and approval. 11/26/2025 Please see comment and update accordingly: PTA-21A "Please include the following AI statement at the end of your response: "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks."	**# of Days - APA Review:**	3

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	12/9/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/9/2025 2:16 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
PTA 01	BLAND, CRYSTAL	11/25/2025	11/25/2025 Per FDA's Email, "The planned ATO date is 12/31/2025."	PIA in Queue (CDRH Division of Mammography Quality Standards).pdf CDRH Division of Mammography Quality Standards Intune_SOP Approved.pdf
PTA 21A	BLAND, CRYSTAL	11/26/2025	Please include the following AI statement at the end of your response: "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks."	