PTA / PIA: FDA - MaaS360 MDM - QTR2 - 2026 - FDA5270489

Created Date: 5/29/2026 6:17 PM Last Updated: 6/11/2026 2:13 PM

General Information

PTA / PIA Name:	FDA - MaaS360 MDM - QTR2 - 2026 - FDA5270489	**PTA / PIA ID:**	4533340
Component Name:	FDA - CTP MaaS360 Enterprise Mobile Device Management	**ATO Boundary Name:**	CTP MaaS360 Enterprise Mobile Device Management
Overall Status:	Complete	**# of Days - Open:**	27
Submitter:		**Submit Date:**	5/29/2026
Next Assessment Date:	06/10/2029	**Expiration Date:**	6/10/2029
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?	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.	4/13/2026
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	Tarun Bhaskaran
PTA 01A:	POC Title and Organization	System Owner FDA/CTP
PTA 01B:	POC Email Address	Tarun.Bhaskaran@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-7898
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Since the latest privacy assessment, the Center for Tobacco Products (CTP) has implemented two changes to the Mobile Device Management (MDM) system. First, CTP established Application Programming Interface (API) read-only access for the Food and Drug Administration (FDA) Cybersecurity team to retrieve device-level data from MaaS360 via the Device Info API for security monitoring and reporting purposes. While the majority of data elements returned by this endpoint are non-Personally Identifiable Information (PII) device characteristics, the endpoint also returns PII elements including the enrolled user's username, email address, device phone number, International Mobile Equipment Identity (IMEI), Unique Device Identifier (UDID), platform serial number, MaaS360 device identification (ID), unified traveler device ID, user domain, and Wi-Fi Media Access Control (MAC) address, which may constitute PII when combined with other identifying data. Second, the FDA Cybersecurity team also retrieves administrator login activity data via the Admin Login Info API, which returns PII elements including administrator usernames, login and logout timestamps, session duration, and Internet Protocol (IP) addresses. The non-PII device characteristics returned by the Device Info API — including device type, manufacturer, model, operating system, compliance status, and enrollment information — are shared with the Department of Health and Human Services (HHS) Cybersecurity team for security oversight and reporting purposes at the departmental level. This downstream sharing is limited strictly to non-PII elements and is governed by enterprise role-based access controls restricted to authorized departmental dashboards. Full details regarding all data elements and their use are provided in this assessment. No other substantive changes to the CTP MaaS360 system have occurred since the last Privacy Impact Assessment (PIA), and this submission represents a routine validation and refresh in accordance with applicable privacy review requirements.
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 Food and Drug Administration (FDA) Center for Tobacco Products (CTP) issues Apple iPhones to state inspectors who perform services under contract agreements with FDA/CTP. These devices enable inspector access to two primary applications: the CTP Tobacco Inspection Management System (TIMS) and the Vape Inspection Application (VIA). Using these iPhones, inspectors transmit inspection data to FDA for analysis and response, where TIMS and VIA are used to schedule and record the results of retail establishment inspections. These inspections focus on monitoring and ensuring establishment compliance with the Family Smoking Prevention and Tobacco Control Act (TCA), particularly as it relates to the improper sale and marketing of

tobacco products.

Due to the large number of issued devices and the geographical distribution of inspectors throughout the United States, CTP must manage these devices and their software remotely. The Mobile Device Management (MDM) system — also known as Mobile as a Service 360 (MaaS360) — provides a cloud-based portal environment to monitor and manage device configuration, inventory, user accounts, and security settings on a 24/7 basis. Critically, this remote management capability means that state inspectors are not required to physically return their devices to CTP for troubleshooting or upgrades, significantly reducing operational burden. MaaS360 also enables CTP to push patches, update configurations, and distribute in-house mobile applications directly to user devices based on each user's assigned role. The in-house mobile applications managed through MaaS360 include the VIA, the Vape Inspection Mobile Training Application (VIMTA), the Mobile Inspection Training (MIT) Application, the Inspection Mobile Training Application (IMTA), and TIMS. MaaS360 Mobile Application Security provides additional data protection for enterprise applications that use the Software Development Kit (SDK) during development and allows for automatic integration of iPhone Operating System (iOS)/Android apps through uploading in-house mobile applications, provisioning profiles, and signing certificates. The MaaS360 Mobile Application Management element further provides the ability to add applications and distribute them to supported devices managed by MaaS360, including through the MaaS360 App Catalog, an on-device application that allows users to view, install, and receive alerts about updated and managed applications.

The system also includes a Mobile Threat Management component that provides enhanced security through mobile malware detection and advanced jailbreak/root detection, allowing FDA/CTP to set and enforce compliance policies around detected security vulnerabilities. In the event a device is reported lost or stolen, MaaS360 enables CTP to remotely place the device into "lost/stolen" mode, locking it down and making its location available to local law enforcement and FDA's Cybersecurity Team. Additionally, the system automatically alerts MaaS360 administrators when a device's cellular service or geographic location falls outside of approved parameters, providing an added layer of security oversight.

There are two primary categories of individuals who interact with MaaS360. The first group consists of System Administrators, who are FDA employees, and TIMS/VIA Help Desk staff, who are FDA Direct Contractors. System Administrators access the MaaS360 portal using Department of Health and Human Services (HHS) user credentials, including HHS/Operating Division (OpDiv) Personal

		Identity Verification (PIV) cards, and are responsible for creating smart group policies, managing user accounts, ensuring device compliance with CTP/FDA Mobile Security Policy, and setting delayed mobile operating system upgrades. Help Desk staff use their credentials to perform functions such as resetting passcodes, remotely wiping devices, distributing in-house mobile applications, and maintaining device ownership data. Access for both groups is granted only with supervisory approval and is governed by role-based, least-privilege principles, with the system access list reviewed on a quarterly basis. The second group consists of federal and state inspectors, who are the primary end users of the CTP-issued iPhones and the TIMS and VIA mobile applications. Notably, these inspectors do not have access to the MaaS360 portal itself — their interaction with the MDM system is limited to the MaaS360 client application loaded on their device, which operates transparently in the background without impacting their user experience. Since the last privacy assessment, CTP has established API read-only access for the FDA Cybersecurity team to retrieve data from MaaS360 via two endpoints for security monitoring and reporting purposes. The first endpoint, the Device Info API, provides device-level data that includes both non-Personally Identifiable Information (PII) device characteristics and certain PII elements associated with the individual to whom each device is assigned. The second endpoint, the Admin Login Info API, provides administrator login activity data that includes PII elements such as usernames, login and logout timestamps, session duration, and IP addresses associated with administrator access to the MaaS360 portal. Access via both endpoints is strictly read-only and does not permit the FDA Cybersecurity team to modify any data or configurations within the MaaS360 system. The non-PII device characteristics returned by the Device Info API are additionally shared with the HHS Cybersecurity team for security oversight and reporting purposes at the departmental level.
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.	MaaS360 collects two categories of information: PII and non-PII device data. With respect to PII, the system collects the name, professional email address, device phone number, International Mobile Equipment Identity (IMEI), Unique Device Identifier (UDID), platform serial number, MaaS360 device ID, unified traveler device ID, user domain, username, FDA property number, and geolocation information of the individual to whom each device is assigned. It is important to note that all collected contact information is professional in nature and does not include any personal or home contact information. This PII is used primarily to identify device ownership and to manage and secure mobile devices in accordance with CTP/FDA policies. Geolocation data specifically serves the purpose of enabling the CTP Help Desk to track the

last known location of devices that are lost or stolen, and to support incident response efforts in coordination with local law enforcement and FDA's Cybersecurity Team.

In addition to PII, MaaS360 collects a range of non-PII device data used to monitor and manage the configuration and status of CTP-issued devices. This includes the device name, device type, manufacturer, model, operating system (OS), installed date, last reported communication with the MaaS360 portal, platform name, compliance status, enrollment information, and managed status. This non-PII data supports the day-to-day administration of the MDM system and helps ensure that all devices remain compliant with CTP/FDA security policies.

Once a device is registered in MaaS360, all collected information is synchronized continuously between the device and the MaaS360 portal, ensuring that data remains current for as long as the user has an assigned device. When a federal or state inspector is terminated, their assigned device is returned to FDA/CTP in accordance with a Standard Operating Procedure (SOP) for the return and data wipe/reset of devices prior to potential re-issue to another user. Disposition authorities for MaaS360 records fall under file code 9995a and National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.1 and 5.2, Data Files Consisting of Summarized Information, under which records may be deleted when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.

MaaS360 shares data with the FDA Cybersecurity team via two API read-only endpoints for security monitoring and reporting purposes. The first endpoint, the Device Info API, returns a range of device-level data elements. The non-PII device characteristics returned by this endpoint — including device type, manufacturer, model, operating system, compliance status, and enrollment information — are shared with the HHS Cybersecurity team for security oversight and reporting purposes at the departmental level. This sharing is limited strictly to non-PII elements and is governed by enterprise role-based access controls restricted to authorized departmental dashboards. In addition to these non-PII elements, the Device Info API also returns PII elements including the enrolled user's username, email address, device phone number, IMEI, UDID, platform serial number, MaaS360 device ID, unified traveler device ID, and user domain. The Wi-Fi Media Access Control (MAC) address is also returned and may constitute PII depending on context, as it can be used in conjunction with other data elements to identify or track an individual. The second endpoint, the Admin Login Info API, returns administrator login activity data including username, login and logout timestamps, session

		duration, Internet Protocol (IP) address, operating system, browser version, and authentication status. Of these elements, username, login and logout timestamps, session duration, and IP address constitute PII, as they are directly linkable to identifiable System Administrators and Help Desk staff. All PII elements shared via both API endpoints are accessible to the FDA Cybersecurity team on a read-only basis and are used solely for security monitoring and reporting purposes, and all PII elements remain within FDA's Operating Division.
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 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.	MaaS360 is a security software tool used by CTP administrators in relation to Tobacco Inspection Management System (TIMS) and Vape Inspection Application (VIA) Help Desk operations. The core features of MaaS360 MDM, as referenced in the Federal Risk and Authorization Management Program (FedRAMP) cloud certification package, include device enrollment, configuration, security policy management, in-house mobile applications, and device actions such as sending messages, locating devices, locking, and wiping. These functions collectively necessitate the collection and maintenance of both PII and non-PII data about two distinct categories of individuals: federal and state inspectors who are the device owners, and System Administrators and Help Desk staff who manage the devices and portal. With respect to federal and state inspectors, MaaS360 collects their name, professional email address, device phone number, International Mobile Equipment Identity (IMEI), Unique Device Identifier (UDID), platform serial number, MaaS360 device ID, unified traveler device ID, user domain, username, FDA property number, and geolocation information. This information is collected solely to identify to whom a specific device is assigned and to enable the secure management of that device in accordance with CTP/FDA policies. Geolocation information is specifically collected so that the CTP Help Desk can assist users with tracking the last known location of devices that are lost or stolen. When CTP receives an Incident Response Lost/Stolen/Personally Identifiable Information (PII) Breach report form and/or a police report from an inspector reporting the theft or loss of a device, CTP immediately sets the device to lost mode, which enables device location information to be made available to local law enforcement and/or FDA's Cybersecurity Team. Additionally, MaaS360 automatically emails MaaS360 administrators on a 24/7 basis when a device's

cellular service is no longer either AT&T or Verizon and/or the mobile country code is not that of an approved area, prompting CTP to remotely place the device in lost/stolen mode and open a support ticket with the FDA Cybersecurity Team and CTP's Information System Security Officer (ISSO) to investigate. It is important to note that while federal and state inspectors are the device owners, they do not have access to the MaaS360 portal itself.

With respect to System Administrators, who are FDA employees, and TIMS/VIA Help Desk staff, who are FDA Direct Contractors, their access to PII within the MaaS360 portal is governed by the least-privilege principle, meaning access is restricted to the minimum amount of information necessary to perform their official duties. System Administrators require access to PII in order to create smart group policies, manage user accounts, ensure device compliance with CTP/FDA Mobile Security Policy and HHS Mobile Apps Privacy Policy, and set delayed mobile operating system (OS) upgrades. Help Desk staff require access to PII in order to perform functions such as resetting passcodes, remotely wiping devices, distributing in-house mobile applications, maintaining device ownership data, and reporting information.

The FDA Cybersecurity team retrieves device-level and administrator login activity data from MaaS360 via two read-only Application Programming Interface (API) endpoints. With respect to device-level data retrieved via the Device Info API, the PII elements returned include the enrolled user's username, email address, device phone number, IMEI, UDID, platform serial number, MaaS360 device ID, unified traveler device ID, and user domain. The Wi-Fi Media Access Control (MAC) address is also returned and is treated as potentially PII given that it can be used in conjunction with other data elements to identify or track an individual. In addition to these PII elements, the Device Info API also returns non-PII device characteristics — including device type, manufacturer, model, operating system, compliance status, and enrollment information — which are shared with the HHS Cybersecurity team for security oversight and reporting purposes at the departmental level, limited strictly to non-PII elements and governed by enterprise role-based access controls. With respect to administrator login activity data retrieved via the Admin Login Info API, the PII elements returned include administrator username, login and logout timestamps, session duration, and Internet Protocol (IP) address. Access to these PII elements is necessary to enable the Cybersecurity team to monitor device-level security posture, detect unauthorized or anomalous login activity, and support incident response activities. All PII elements shared via both endpoints are used solely for security monitoring and reporting purposes and

		remain within FDA's Operating Division.
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?	Yes
PTA 14A:	Is the mobile application HHS developed and managed or a third-party application?	HHS
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.	MaaS360 manages a total of seven mobile applications that support CTP's Tobacco Inspection Management Program (TIMP). Five of these are in-house mobile applications developed to support tobacco inspection operations, while two are applications used specifically to monitor and manage mobile devices through the MaaS360 portal. The five in-house TIMP mobile applications and their respective purposes are as follows. The Vape Inspection Application (VIA) provides a method for electronically capturing information related to vape inspections conducted at retail establishments. The Vape Inspection Mobile Training Application (VIMTA) provides and tracks training of inspectors who use the VIA. The Mobile Inspection Training (MIT) Application serves as an interactive tutorial for Undercover Underage Purchasers to prepare them for the Tobacco Retail Compliance Check Inspection Program. The Inspection Mobile Training Application (IMTA) provides and tracks training of inspectors who use the Tobacco Inspection Management System (TIMS). Finally, TIMS provides a method for electronically capturing information related to Undercover Buy (UB) and Advertising and Labeling Inspections. The two device management applications are the MaaS360 App and the App Catalog. The MaaS360 App enables devices to send and receive commands from the MaaS360 portal for actions such as enforcing security policies, enrolling devices, sending notifications, retrieving device information, wiping devices, and pushing in-house mobile applications. The App Catalog lists available TIMP mobile applications based on the user's assigned role, allowing users to download or update mobile applications when directed to do so by CTP/TIMP Help Desk staff. Access to the mobile applications is role-based and varies depending on the category of user. Federal and state inspectors, including FDA commissioned inspectors and State and Prime Contractor (PC) inspectors, are the primary end users of the five TIMP in-house mobile applications. Their access is limited to the applications relevant to their assigned inspection duties, as determined by their role within the system. System Administrators, who are FDA employees, and TIMS/VIA Help Desk staff, who are FDA Direct Contractors, manage and oversee the mobile applications through the MaaS360 portal. These individuals are responsible

		for distributing, updating, and maintaining the applications on user devices. Federal and state inspectors access the TIMP mobile applications directly on their CTP-issued iPhones. The App Catalog application, which is managed through the MaaS360 portal, presents each inspector with the specific applications available to them based on their assigned role. When directed by CTP/TIMP Help Desk staff, inspectors can download or update their mobile applications through the App Catalog. The MaaS360 App operates in the background on each device, transparently managing device security and configuration without significantly impacting the inspector's user experience. System Administrators and Help Desk staff access and manage the mobile applications through the MaaS360 cloud-based portal, using their HHS or non-HHS user credentials, including HHS/Operating Division (OpDiv) Personal Identity Verification (PIV) cards or a password and email address combination, to authenticate and perform their respective administrative functions.
PTA 16:	Does the mobile application have a privacy notice?	Yes
PTA 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
PTA 18:	Does the mobile application use measurement and customization technology?	No
PTA 19:	Does the mobile application have any information directed at children under the age of thirteen?	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 Contact Information Email 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.	FDA Property Number Geolocation Information IMEI Phone Number (Device) UDID (Unique Device Identifier) Platform Serial Number MaaS360 Device ID Unified Traveler Device ID (unifiedTravelerDeviceId) User Domain (userDomain) Wi-Fi MAC Address Email Address (Device Info API) Administrator Login Activity – Username Administrator Login Activity – Timestamps and Session Duration Administrator IP Address Enrolled User Username
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.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose for which PII is collected and used in MaaS360 is to identify to whom a specific device is assigned and to manage and secure mobile devices in accordance with CTP/FDA policies.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The PII elements shared with the FDA Cybersecurity team via the Device Info API and Admin Login Info API for security monitoring and reporting purposes, as previously described, represent the only secondary use of PII maintained within the MaaS360 system.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The legal authority governing the MaaS360 system and its associated mobile applications — including TIMS, MIT, IMTA, VIMTA, and VIA — is the Federal Food, Drug, and Cosmetic Act, as Amended by the Family Smoking Prevention and Tobacco Control Act (TCA), 21 U.S.C. secs 301-399. Specifically, Section 103 of the TCA directs that, to the extent feasible, the Secretary shall contract with the States to carry out inspections of retailers for the enforcement of the Act.
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 Phone Government Sources Within the OPDIV 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.	An Office of Management and Budget (OMB) information collection approval number is not required because CTP's Mobile Device Management system is a tool used internally by the center. As an internal tool, it does not have any Paperwork Reduction Act (PRA) implications, which is the primary basis for requiring an OMB information collection approval number.
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 provide their professional contact information as a practical requirement to communicate with FDA about submissions. There are no opt-out procedures specific to MaaS360. While FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity, providing a degree of flexibility in terms of whose PII is collected.

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 major changes to the MaaS360 system with respect to the collection or handling of PII are currently planned or anticipated. However, if FDA does change its practices regarding the collection or handling of PII related to the MDM system, the agency will adopt measures to provide any required notice and obtain consent from affected individuals. The methods through which FDA would notify individuals and obtain consent include sending emails directly to affected individuals, updating the applicable Rules of Behavior to reflect any changes, or utilizing other available means to inform individuals of any changes to how their PII is collected or used.
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.	Several channels are available to individuals who believe their PII has been inappropriately obtained, used, or disclosed, or who believe their PII is inaccurate. Individuals may contact the CTP, TIMS, or VIA Help Desk by phone, mail, or email using the contact information provided on fda.gov. They may also contact FDA's Privacy Office or the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) to raise their concerns. Additionally, individuals have the option of raising concerns and/or submitting data corrections through supervisory channels and through the FDA's Employee Resource and Information Center (ERIC). Taken together, these multiple avenues ensure that individuals have accessible and varied means through which they can raise concerns about the handling of their PII or request corrections to inaccurate information maintained within the MaaS360 system.

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 following processes are in place to ensure the integrity, availability, accuracy, and relevancy of PII maintained within the MaaS360 system: Individuals are informed of the PII collected about them at the time of device issuance and are responsible for providing accurate professional information. Accuracy is further supported by FDA personnel's ability to correct and update information directly within the system, providing an additional mechanism for maintaining accurate records. The relevancy of PII is ensured by the design of the system itself, which limits the PII collected to only that which is necessary for device management and security purposes. Additionally, the agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and to delete unneeded accounts from the system, ensuring that only current and relevant PII is maintained. Both integrity and availability are protected through the administrative, technical, and physical privacy and security controls implemented for the system. These controls are selected based on National Institute of Standards and Technology (NIST) guidance, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199 and NIST Special Publication (SP) 800-53, ensuring that PII maintained within MaaS360 is protected against unauthorized access, alteration, or loss and remains available to authorized users when needed
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.	Users (Federal and State Inspectors): Access to PII is necessary for the purpose of tracking who uses the CTP-issued devices. Since each device is assigned to a specific individual, PII such as the device owner's name, username, and contact information is needed to maintain accurate records of device ownership and assignment. Administrators (FDA Employees): System Administrators require access to PII in order to manage devices, security profiles, and mobile applications across the MaaS360 portal. This includes creating and managing user accounts, enforcing security policies, and ensuring that devices and applications are properly configured and distributed to the appropriate users based on their assigned roles. Contractors (FDA Direct Contractors): TIMS/VIA Help Desk staff require access to PII in order to perform troubleshooting and support functions on behalf of device users. Specifically, this includes tasks such as resetting passcodes, remotely wiping data from a device, and reinstalling mobile applications. PII such as the device owner's name, username, and device identifiers is necessary for Help Desk staff to accurately identify and locate the correct device when performing these support functions. FDA Cybersecurity Team: The FDA Cybersecurity team requires read-only access to specific PII elements returned by the Device Info API and Admin Login Info API. Access to device-level PII — including enrolled user username, email address, device phone number, IMEI, UDID, platform serial number, MaaS360 device ID, unified traveler device ID, user domain, and Wi-Fi MAC address — is necessary to monitor device security posture, identify anomalous device behavior, and support incident response activities. Access to administrator login activity data — including administrator username, login and logout timestamps, session duration, and IP address — is necessary to monitor access patterns, detect unauthorized or anomalous login activity, and support security oversight of the MaaS360 portal. In addition, non-PII device characteristics returned by the Device Info API — including device type, manufacturer, model, operating system, compliance status, and enrollment information — are shared with the HHS Cybersecurity team for security oversight and reporting purposes at the departmental level, limited strictly to non-PII elements and governed by enterprise role-based access controls. All access to PII by the FDA Cybersecurity team is strictly read-only and is limited to the minimum information necessary to fulfill its security responsibilities.

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 who require access to the MDM system must first have a valid network account. Prior to being granted access, these individuals must obtain supervisory approval and a supervisory signature on the MDM user account creation form. The relevant supervisor is also responsible for indicating on this form the minimum level of access required for the user to complete their job duties, ensuring that access is granted in accordance with the least-privilege principle. Once access has been granted, the agency conducts periodic reviews of the system access list on a quarterly basis. During these reviews, users' access roles and permissions are adjusted as needed and any unneeded accounts are deleted from the system. This quarterly review process ensures that only individuals with a current and legitimate need to access PII are permitted to do so, and that access rights remain aligned with each user's official duties over time.
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 technical enforcement of access controls is achieved through a role-based access control framework. When a new user account is created, the relevant supervisor is required to indicate on the MDM user account creation form the minimum level of access required for the user to complete their job duties. Access is then configured within the system based on role-based criteria, ensuring that each user can only access the specific information and functions necessary for their assigned role. For example, Help Desk staff are granted access to the functions and PII necessary to perform troubleshooting tasks such as resetting passcodes and wiping devices, while System Administrators have access to the broader set of functions needed to manage devices, security profiles, and mobile applications across the MaaS360 portal. This role-based access control approach ensures that no user is granted broader access to PII than is necessary for their official duties, thereby minimizing the risk of unauthorized access to or misuse of PII maintained within the MaaS360 system.
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 are required to complete annual mandatory computer security and privacy awareness training. This training covers Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability, as well as the proper handling of data, including any special restrictions on data use and/or disclosure. Completion of this training is verified by the FDA Office of Digital Transformation (ODT), which confirms that all FDA employees and Direct Contractors have successfully completed the required training.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	System users receive two additional forms of training above and beyond the general security and privacy awareness training required of all FDA employees and Direct Contractors. First, personnel are trained on the specific use of the MaaS360 system itself, ensuring that users understand how to properly operate the system in accordance with CTP/FDA policies and procedures. Second, all system users are required to review the Rules of Behavior associated with the MaaS360 system, which outlines the specific responsibilities and expectations for individuals who have been granted access to the system and the PII it maintains. Additionally, for those system users who require further guidance on privacy-related matters beyond what is covered in the general awareness training and system-specific training, additional role-based privacy training is made available through FDA's Privacy Office. This ensures that users with more specialized privacy responsibilities have access to the targeted training necessary to fulfill those responsibilities effectively.
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).	Disposition authorities for the applications' records fall under file code 9995a, as well as National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.1 and 5.2, Data Files Consisting of Summarized Information. Under this schedule, records may be deleted when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. Some outputs such as documents and memos are captured in the CTP Case Management System (CCMS), while others are only found in VIA and are referenced there by the Office of Compliance and Enforcement (OCE). The applicable file codes for VIA records are as follows: CTP-2110: Tobacco Retailer Inspection Case Files CTP-2121: Tobacco Establishment Inspection and Investigation Review Memos — No Action Indicated (NAI) and Voluntary Action Indicated (VAI) CTP-2122: Tobacco Establishment Inspection and Investigation Review Memos — Official Action Indicated (OAI) CTP-2210: Tobacco Internet Surveillance or Inspection Activity Files — NAI and VAI CTP-2120: Tobacco Internet Surveillance or Inspection Activity Files — OAI

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, which encompasses the annual mandatory computer security and privacy awareness training required of all FDA employees and Direct Contractors, as well as system-specific training on the MaaS360 system and the provision of a user manual to assist users through training exercises and provide guidance regarding different system functionalities. System documentation is also in place to advise users on the proper use of the system. Additionally, the Need to Know and Minimum Necessary principles are implemented when awarding access to the system, ensuring that users are only granted access to the PII necessary to perform their official duties. Supervisory approval and signature are required before access is granted to any user, and the system access list is reviewed on a quarterly basis to adjust roles and permissions and delete unneeded accounts. Technical safeguards include role-based access settings, which restrict each user's access to the minimum amount of information necessary to perform their job duties. The FDA Cybersecurity team's access to MaaS360 data is governed through two read-only API endpoints — the Device Info API and the Admin Login Info API — which provide device-level and administrator login activity data respectively for security monitoring and reporting purposes. The Device Info API returns both PII elements — including enrolled user username, email address, device phone number, IMEI, UDID, platform serial number, MaaS360 device ID, unified traveler device ID, user domain, and Wi-Fi MAC address — and non-PII device characteristics, including device type, manufacturer, model, operating system, compliance status, and enrollment information. The non-PII device characteristics are shared with HHS for security oversight purposes. The read-only nature of this access ensures that the Cybersecurity team can retrieve data without the ability to modify, delete, or otherwise alter any data or configurations within the MaaS360 system, consistent with the least-privilege principle. Physical safeguards for the MaaS360 system are provided through the cloud service infrastructure maintained by the system's cloud service provider, which operates in accordance with Federal Risk and Authorization Management Program (FedRAMP) authorization requirements. These physical controls include, but are not limited to, secured data center facilities with access controls, environmental protections, and continuous monitoring to protect the hardware and infrastructure supporting the MaaS360 system and its associated PII against unauthorized physical access, environmental hazards, and other physical threats. Additional appropriate physical controls have been selected from NIST SP 800-53, as determined using FIPS 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/29/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/29/2026
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/10/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/10/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	12

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/11/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	1

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/11/2026 11:10 AM	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				