PTA / PIA: OS - O365 - QTR3 - 2025 - OS3074757

Created Date: 9/4/2025 1:01 PM Last Updated: 9/4/2025 6:03 PM

General Information

PTA / PIA Name:	OS - O365 - QTR3 - 2025 - OS3074757	**PTA / PIA ID:**	3753826
Component Name:	OS - OS - HHS Office 365	**ATO Boundary Name:**	HHS Office 365
Overall Status:	Complete	**# of Days - Open:**	1
Submitter:		**Submit Date:**	9/4/2025
Next Assessment Date:	09/03/2028	**Expiration Date:**	9/3/2028
Office:		**OpDiv:**	OS
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?	Yes
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.	11/10/2025
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	Michael Elkins
PTA 01A:	POC Title and Organization	IT Specialist (InfoSec) OCIO-Operations
PTA 01B:	POC Email Address	michael.elkins@hhs.gov
PTA 01C:	POC Phone Number	202-815-1969
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.	Microsoft Co-Pilot has been added to the environment.
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.	Health and Human Services (HHS) established the HHS Office 365 (Office 365) as a cloud computing Software as a Service (SaaS) solution for email, collaboration, and communication leveraging the Federal Risk and Authorization Management Program (FedRAMP) Microsoft Government-only O365 SaaS. Within Core Services, there is also accompanying support architecture to support identity management. This support architecture includes the following elements: MS Active Directory Federation Services, MS Active Directory Federation Services Proxy and MS Directory Synchronization. Trellix and Microsoft Exchange Online Protection/Defender handle the mail filtering, spam protection and anti-malware protection. MS Exchange Online Protection/Defender is specific tool that provides anti-malware and URL filtering protection. These supporting elements are also referred to as the Integration Infrastructure.
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 HHS Office 365 system or connected O365 Applications do not collect or request specific Personally Identifiable Information (PII) data; however, there is a possibility of the exchange of PII data between individuals or groups of individuals through the transmission of e-mail messages. These messages could be stored for retrieval in a user's mailbox or personal archives indefinitely. Litigation Hold requests from appropriate authorities that result in legal investigations will result in the system retaining data per legal investigation requirements. E-mails are transmitted between HHS employees for normal day to day business operations, but PII data is never explicitly collected or used by the system (i.e., there are no forms or fields for PII collection, and PII collection is not the explicit purpose of the system). The HHS Office 365 system itself does not include an Active Directory server within its Authority to Operate (ATO) boundary, but interconnects to the existing Active Directory infrastructure to manage and authenticate a user's access to their mailbox(s). As a result, Active Directory field data requirements are managed by the Enterprise Network Management System (ENMS) General Support System rather than the HHS Office 365 system, but HHS Office 365 will synchronize with Active Directory and may maintain this information.
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.	Enterprise Network Management System (ENMS)

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.	HHS Office 365 will synchronize with Active Directory and may maintain this information. This information typically includes User Principal Name, first, middle, and last name, mailing address, device identifiers, organization, office number, email address and phone number. This information is collected as part of the need for the user to access the system and use with the various applications to communicate and collaborate with others.
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).	http://office.com
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
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 Website provides an access to additional non-core applications that are restricted to web-based access. Noted non-core applications: Microsoft List, Microsoft To-Do. Additionally, the Web Interface serves as alternate interface for Core Applications
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?	Yes
PTA 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
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.	Mobile application/s provides access to additional non-core applications that are restricted to web-based access. Noted non-core applications are: Microsoft List, Microsoft To-Do. Additionally, the mobile Interface serves as alternate interface for Core Applications.
PTA 16:	Does the mobile application have a privacy notice?	No
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?	Yes

PTA 21A:	What are the AI tools and how are they used?	Microsoft Copilot, Copilot Chat has been deployed to the GSA FedRAMP package by the vendor and is available for all OCIO-Ops users through our FedRAMP Package. No other AI Tools deployed

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.	Identifying Numbers Device Identifiers Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
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 Members of the public 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.	10,000 – 49,999

PIA 25:	For what primary purpose is the PII used?	HHS O365 system uses the Enterprise Network Management System (ENMS) Active Directory credential information (primarily the User Principal Name, User ID and authenticator. This is used by the system for authentication purposes only. The HHS Office 365 system may also access additional information stored in the ENMS Active Directory such as electronic address information, but this information is defined by the GSS (general support system) and not needed by the HHS Office 365 system. In addition to ENMS interface the O365 System has deployed Microsoft Copilot as an AI tool that can interact with the O365 user created and maintain PII/PHI and other sensitive data. Copilot's noted purpose is to be used to extract data from Documents supplied by the user to create revisions to other documents or new documentation and is expected to reduce the amount of time required to complete tasks. This includes writing tasks, coding tasks, spreadsheet tasks, etc. Microsoft Copilot as an AI tool can interact with user created and maintain PII/PHI and other sensitive information, however due to the O365 Data Loss Prevention Policies and Microsoft own configurations the Copilot AI tool cannot be trained using the PII collected in the system. The uses of Personally identifiable information (PII) are as varied as the functions and activities of HHS. Uses could include determination of benefits, health care payment, treatment or operations; conduct of health-related research; internal administrative and human resources functions; conduct of background checks; disciplinary actions; certification of health care service providers; or any of dozens of other activities Health & Human Services (HHS) conducts. The O365 Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	No root-level or administrative users will have access to all the PII in this system. It is conceivable that HHS will employ some form of data loss prevention or discovery tool to identify PII contained in e-mails for purposes of complying with a discovery request or evaluating its privacy and security practices.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	42 US Code, The Public Health and Welfare. This is the Title of the US Code that implements HHS and provides it with the legal authority to operate.
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 In-person Hard Copy Mail/Fax Phone Email Online Government Sources Within the OPDIV Other HHS OPDIV Other Federal Entities Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet Private Sector
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.	Not Applicable - OMB Control Numbers are used for data collections subject to the PRA & does not apply to instrumentalities, which is applicable to O365 in this case.
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.	Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	The uses of Personally identifiable information (PII) are as varied as the functions and activities of HHS. Uses could include determination of benefits; health care payment, treatment or operations; conduct of health-related research; internal administrative and human resources functions; conduct of background checks; disciplinary actions; certification of health care service providers; or any of dozens of other activities Health & Human Services (HHS) conducts. Enterprise Network Management System (ENMS) Active Directory credential information (primarily) the User Principal Name, userID and authenticator) is used by the system for authentication purposes only. This data is only shared with the OPDIV that have accounts within system.
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)).	MOU with ENMS.

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.	In the event of PII disclosure the OCIO-Operations Service Desk is notified to create a ticket for HHS incident response (IR) to investigate disclosure.
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 requires user credentials for system authentication for all users. If a user opt-out request is received/granted, the user cannot be authenticated and will be removed from system access. PII data specifically collected through the use of an HHS Office 365 system; is managed by the OPDIV Policy and Regulations that collects and manages that information, therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes managed by the supported OPDIV. Any PII data contained in an e-mail message, presented to Microsoft CoPilot is only shared with the user(s) whom receive the e-mail or user that uploads data to Microsoft CoPilot.
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.	HHS O365 has a required warning banner advising users that when they are accessing HHS O365 that the system is specifically collecting PII as part of the use and/or access of the O365 system and O365 applications (i.e. CoPilot, Teams etc.). Therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of HHS Office 365
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.	There is a department-wide process. Individuals would not be likely to discover concerns through the use of PII in the HHS Office 365 system, but through the underlying business processes avenues for redress which would include contacting the operations centers, help desks or customer service providers of those individual business operations. Members of the public could also avail themselves of the Freedom of Information Act (FOIA) or Privacy Act for redress services. For issues with PII detected by HHS staff members, individuals can also report suspected fraud, breaches, or other issues to the Computer Security Incident Response Center (CSIRC) or to the business process owner.

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.	Data integrity is maintained at the level of the business process, through maintenance of the applications that support business processes and Data Loss Prevention (DLP) Settings/Policies. Review of PII in the Email, MS Teams and CoPilot Services would not be efficient or appropriate. All messages, headers attachments, and CoPilot requests may be reviewed and sorted through the use of predefined search options, including key word search, to support security incident response, data loss prevention, or e-discovery.
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 are granted access to communicate and collaborate with others. Administrators to manage, restore services, and for authorized purposes such as e-discovery or detection of breaches. Contractors in the management of the HHS O365 Cloud Services.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only users (i.e., those authorized to send and receive e-mails, MS Teams Communcations and CoPilot requests) and administrators are able to access the contents of e-mails MS Teams Comms and CoPilot requests. The cloud service providers will be prevented from accessing contents using encryption standards, and accessing the content will not be part of the services provided. HHS employees and contractors must have completed the personnel screening process and corresponding forms and documents are provided accounts as part of their employment package, and these accounts are accessed through HHS Office 365. HHS Office 365 Administrators are approved by the Program Manager, and must complete necessary Network Access Request forms and training to obtain the elevated privileges required for administrative duties. The HHS Office 365 administrator must also register and request access, and sign corresponding Non-Disclosure Agreements, to the Microsoft Administration Portal for access to the management interface for the cloud-based components

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.	This is a standard e-mail system, and e-mails are sent from a user to a specified recipient(s). Individuals that were not included on an e-mail communication will not have access to any e-mails that are not specifically addressed to them. MS Teams messages sent from a user to a specified recipient(s). Individuals that were not included on a message communication will not have access to any message that are not specifically addressed to them. MS CoPilot includes multiple protections to block harmful content, detect protected material, and prevent prompt injections. The Microsoft cloud providers in particular are not expected to have any access to the content of HHS email transmissions. HHS Office 365 System Administrators with the appropriate Exchange permissions, who have signed the Privileged User Rules of Behavior (RoB) and performed the required Role Based training are able to access the contents of emails, only for authorized purposes such as e-discovery or detection of breaches.
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 users are required to complete annual Information Security Training and Privacy Awareness Training. All system administrators and managers are required to complete the annual Role-Based Training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	All Users will be provided training regarding the basic concepts of accessing accounts and collaboration services offered by the HHS Office 365 cloud-based solution. HHS Office 365 Administrators are required to complete training in Security Incident Response, Contingency Planning and Operations, and Role Based training. HHS may mandate additional training; however, this would be out of scope for the HHS O365 system PIA to address.
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).	User can archive messages containing PII data within the MS One Drive or in their mailbox indefinitely. There is no data retention policy set up for HHS Office 365. If a user deletes a message, at which time it is moved to the Deleted Items Recovery folder for 30 days. After this period, the deleted mail is stored in a purge folder for 30 days, during which time only authorized administrators can access it. After the 30-day time period of being in the purge folder the email is permanently deleted and is no longer accessible to HHS Office 365 Administrators. Litigation Hold requests from appropriate authorities that result in legal investigations will result in the system retaining data per legal investigation requirements.

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.	HHS Office 365 implements security controls to protect PII, as defined by Office of Management and Budget mandates, the Federal Information Security Management Act (FISMA), and NIST Special Publications (SP) 800-53, 800-37, 800-122, NIST Federal Information Processing Standards (FIPS) 200, 201, 199, 197, 140-2, and other associated documents as outlined by Federal Risk and Authorization Management Program (FedRAMP) (www.fedramp.gov). This includes achieving and maintaining an ATO. PII will be secured within the system through the use of administrative controls in the form of: Mandatory security awareness and privacy training for all users. Role-based training for privileged users. Personnel screening as required by HHS. Completion of contractual agreements and Rules of Behavior. Users can encrypt email traffic, including those containing PII, in accordance with applicable HHS policies. Technical controls include Role-based access controls based on Active Directory permissions to obtain authorized access to the system. All user logins will be logged, with auditing performed as part of the HHS Office 365 Continuous Monitoring program. Spam and email content filtering. Anti-malware software installed on HHS Office 365 servers. FIPS 140-3 compliant encryption of data in transit. Restricted access to the GCC through the HHS Trusted Internet Connection (TIC) Access Points. Information Flow Control through the use of firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Data Loss Prevention (DLP) and Continuous Data Protection (CDP) policy that allows for direct remote Operating Division (OpDiv) administration. Non-repudiation through support of digital signatures and encrypted email, using PIV and other types of digital certificates. Physical controls include Hosting within data centers which control and monitor physical access to the system components, including visitor control and auditing of access records. Protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/4/2025
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	9/4/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	9/4/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 9/4/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	9/4/2025
SAOP Review Comments:	Approved on behalf of the SAOP	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
9/4/2025 1:22 PM	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 04	BLAND, CRYSTAL	9/4/2025	On the next iteration of the PTA please include the AI statement in your response. While it is mentioned later on in the PIA in PIA-25, it is better to mention it upfront.	