US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2026

OPDIV:

NIH

Name:

NIH Microsoft 365

PIA Unique Identifier:

P-1123318-600080

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

NIH Microsoft 365 (M365) is productivity software, collaboration and cloud-based services owned by Microsoft. NIH M365 provides licenses to desktop and mobile software, and hosted email and intranet services. M365 is used by the Institutes, Centers, and Offices (ICOs) at the NIH to facilitate greater collaboration with internal and external stakeholders, in a secure Federal Risk and Authorization Management Program (FedRAMP) approved cloud environment. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

M365 includes the following application suites and maintain their own unique privacy threshold analysis (PTA), with all legal authorities documented.

M365 Enterprise:
Microsoft Office - Word, Excel, One Note, Power Point Exchange - Mail, Calendar, People Tasks, To-Do,

Video Portal - (Stream) a cloud-based video storage and streaming solution,
Viva Suite - (Insights) an employee engagement and business performance tool using artificial intelligence (AI), analytics, and process insights,
Microsoft 365 Copilot is an AI-generated assistant integrated across M365 applications which enhances productivity by streamlining tasks and generating intelligent content,
Microsoft 365 Copilot Chat helps users draft emails in Outlook, create content in Word, summarize files, analyze Excel data, generate visuals, handle meeting notes in Teams, and can deploy AI agents for tasks like monitoring inboxes or automating workflows.

AI use cases can include transcription, summaries of meetings or data, creating draft documents, summarizing multi day conversations, and asking work-related questions. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks

M365 Power Platform Services:
Power Business Intelligence (BI) is a business analytics tool that transforms data from multiple sources into interactive visualizations and reports for data-driven decision making,
Power Automate (formerly Flow) is a cloud-based automation tool that creates workflows between apps and services to automate repetitive tasks and business processes without coding,
Power Applications (Apps) is a low-code/no-code platform that enables users to build custom business applications for web and mobile without extensive programming knowledge.

M365 Collaboration Services:
Teams is a collaboration platform that combines workplace chat, video meetings, file storage, and application integration into a unified communication hub for organizations,
Yammer is an enterprise social networking platform that enables employees to collaborate, share knowledge, and communicate across departments and organizations,
SharePoint Online is a web-based collaboration platform that provides document management, intranet portals, file storage, and content management for organizations to share and manage information securely,
OneDrive for Business is Microsoft's enterprise cloud storage solution that provides secure file storage, sharing, and synchronization with advanced administrative controls, compliance features, and larger storage capacity for organizations,
Forms is a survey and quiz creation tool that enables users to easily build forms, polls, and questionnaires to collect feedback and data with automatic response analysis,
Planner is a task management tool that helps teams create plans, organize and assign tasks, share files, and track project progress through visual boards,
Whiteboard is a digital collaborative canvas that allows teams to brainstorm, draw, and ideate together in real-time across devices,
Scheduling (Booking) allows customers to schedule meetings and services while automatically managing staff calendars and sending confirmations.

The NIH M365 is operated and managed by Center for Information Technology (CIT) Unified Communication and Collaboration (UCC) and CIT Hosting and Storage S

Describe the type of information the system will collect, maintain (store), or share.

The type of data and information that NIH M365 will collect, maintain, and/or share includes:
Name
Driver's license number
Mother's maiden name
Email
Phone

Education records
Medical Notes
Certificates

Military status
Taxpayer Identification (ID)
Date of Birth (DOB)
Photographic identifiers
Vehicle identifiers including license plate information
Mailing address
Financial Account Information
Legal documents
Device identifiers
Employment status
Passport number
Demographic data
Employee Records
Training records
Insurance Information
Sensitive network and system data/information.
System vulnerability and compliance information
NIH third-party proprietary information

Data content that are prohibited include:
Executable files with extensions of .exe, .jar, .dmg, .pkg, .msi, and .war
Social Security Number (SSN), including last 4 digits
Credit Card (CC) number
Medical record number (MRN)
Grant and Contract information that is not publicly available

The NIH M365 is not the source system or system of record for personally identifiable information (PII). This Privacy Impact Assessment (PIA) acknowledges only that PII may be present within the M365 Enterprise as a downstream or enabling service; it does not authorize the initial collection, creation, or use of PII.

Responsibility for ensuring appropriate authorization, consent, legal authority, and implementation of required privacy and security controls for any PII (including sensitive PII) that is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of resides with the relevant NIH ICO.

These responsibilities, including applicable legal authorities, PIA development, and privacy controls, are with the ICOs' source systems or source records, or at the point of collection when the information does not originate from an information system.

CIT has implemented the following security safeguards:
NIH Firewall protection
Multi-factor authentication (MFA) requiring more than one method to verify the user's identity.
Security scanning and alerts using data loss prevention (DLP) technologies for PII.

User Access
NIH users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, with all legal authorities documented. The purpose of the IAM is to authenticate and authorize all users and computers in a Windows domain

type network assigning and enforcing information security policies for all computers and installing or updating software. The IAM collects unique usernames and passwords (user credentials) and stores them in an encrypted format. The IAM is an essential service which facilitates and governs network access to various resources.

For individuals external to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user's login credentials. NIH Federated login enables users to use a single authentication method via an individual's parent organization. After the system owner approves access to an individual and registers their parent organization's identity provider, individuals are redirected to their parent organization's identity provider for credentials. NIH Federated Services resides within the Identity, Credential, and Access Management (IAM) Services.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

NIH M365 is used by NIH ICOs to facilitate collaboration with internal and external stakeholders, in a secure FedRAMP approved cloud environment. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

NIH M365 includes the following application suites:
M365 Enterprise
M365 Power Platform Services
M365 Collaboration Services

The type of data and information that NIH M365 can collect, maintain, and/or share includes:
Name
Driver's license number
Mother's maiden name
Email
Phone
Education records
Medical Notes
Certificates

Military status
Taxpayer ID
DOB
Photographic identifiers
Vehicle identifiers
Mailing address
Financial Account Information
Legal documents
Device identifiers
Employment status
Passport number
Demographic data
Employee Records
Training records
Insurance Information
Sensitive network and system data/information.
System vulnerability and compliance information

NIH third-party proprietary information

Data content that are prohibited include:
Executable files with extensions of .exe, .jar, .dmg, .pkg, .msi, and .war
SSN, including last 4 digits
CC number
MRN
Grant information that is not publicly available

The NIH M365 is not the source system or system of record for PII. This PIA acknowledges only that PII may be present within the M365 Enterprise as a downstream or enabling service; it does not authorize the initial collection, creation, or use of PII.

Responsibility for ensuring appropriate authorization, consent, legal authority, and implementation of required privacy and security controls for any PII (including sensitive PII) that is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of resides with the relevant NIH ICO.

These responsibilities, including applicable legal authorities, PIA development, and privacy controls, are with the ICOs' source systems or source records, or at the point of collection when the information does not originate from an information system.

CIT has implemented the following security safeguards:
NIH Firewall protection
MFA requiring more than one method to verify the user's identity.
Security scanning and alerts using DLP technologies for PII

User Access
NIH users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

For individuals external to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services which resides within the IAM Services.

M365 is operated and managed by CIT UCC and CIT HSS.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth
Name
Photographic Identifiers
Driver's License Number
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Financial Accounts Info
Certificates

Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Passport Number
Taxpayer ID
Demographic data, Employee Records, Training records, Insurance Information
Sensitive network and system data/information, System vulnerability and compliance information
NIH third-party proprietary information

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The information is used for collaborative research, training, human resources (HR) management, business administration and management.

Describe the secondary uses for which the PII will be used.

NA

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 301 and 302, 44 U.S.C. 3101 and 3102, Executive Order 9397;
5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347;
42 U.S.C. 241, 242, 248, 281, 282, 284, 285a, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285l, 285m, 285n, 285o, 285p, 285q, 287, 287b, 287c, 289a, 289c

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

OPM GOVT-1, General Personnel Records

09-25-0099 Clinical Research: Patient Medical Records

09-90-0024 - Financial Transactions of HHS Accounting and Finance Offices

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Email
Online
Government Sources
Within the OPDIV

Identify the OMB information collection approval number and expiration date

0925-0001 - Expiration Date: 12-31-2027
0925-0002 - Expiration Date: 11/30/2027

Other HHS OpDiv
State/Local/Tribal
Other Federal Entities
Non-Governmental Sources
Public
0925-0670 - Expiration Date: 04-30-2026
Private Sector
3206-0182 - Expiration Date: 08/31/2026
1615-0047 - Expiration Date: 005-31-2027

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

NIH M365 is a FedRAMP approved cloud environment which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Users who leverage these services are not share or disclose sensitive or PII data unless that data is accounted for within a security authorization boundary, separately assessed for privacy and security compliance, and has its own PIA.

Describe the procedures for accounting for disclosures.

NIH M365 is used for collaboration and storage. Audit logs are be used to disclose what information is shared and tracked outside of HHS.
Security scanning and alerts using DLP technologies for PII.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Personal information is not collected directly from individuals unless accounted for within a security authorization boundary, separately assessed for privacy and security compliance, and has its own PIA.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Personal information is not collected directly from individuals unless accounted for within a security authorization boundary, separately assessed for privacy and security compliance, and has its own PIA.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Personal information is not collected directly from individuals unless accounted for within a security authorization boundary, separately assessed for privacy and security compliance, and has its own

PIA.

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.

Individuals can contact their ICO Privacy Coordinator or the NIH Senior Official for Privacy at Privacy@mail.nih.gov.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. CIT uses DLP technologies for daily security scanning and alerts for unauthorized PII.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

All NIH M365 development and management staff (employees and direct contractors) have appropriate role-based training for the position's sensitivity level. Background investigations are conducted according to their assigned position.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Access to PII is assigned to personnel based upon current job responsibilities. The system uses specific login information (NIH IAM Services) to assign permissions/user roles.

A two- factor authentication is always used when accessing the system. All administrative staff will sign and comply with the system administrator rules of behavior to ensure HHS and NIH operational policies are followed regarding administrator privileges and technical use for systems and applications.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Personnel with administrator and security related duties must complete the appropriate role-based training upon hire and then annually, which includes content for protecting sensitive information including PII.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the National Archives and Records Administration (NARA) Disposition Authority (DAA) General Records Schedule (GRS).

GRS 5.1: Common Office Records
Disposition: Temporary. Destroy when business use ceases. DAA-GRS 2016-0016-0001

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.
Item 03-008: Clinical Care Administrative Support Records
Disposition: Destroy when 3 years old, but longer retention is authorized if needed for business use. DAA-0443-2018-0002-0001

Item 05-101: Financial Management and Reporting
Disposition: Destroy when 3 years old, but longer retention is authorized if needed for business use. DAA-GRS-2016-0013-0001

Item 06-102: Position descriptions -- Official record copy of position description.
Disposition: Destroy 2 years after position is abolished or description is superseded, but longer retention is authorized if required for business use. DAA-GRS-2014-0002-0002

Item 06-107: Job vacancy case files -- Records of one-time competitive and Senior Executive Service announcements/selections.
Disposition: Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later. DAA-GRS-2014-0002-0006

Item 06-108: Job vacancy case files -- Records of standing register competitive files for multiple positions filled over a period of time.
Disposition: Destroy 2 years after termination of register. DAA-GRS-2014-0002-0007

Item 06-109: Job application packages.
Disposition: Destroy 1 year after date of submission. DAA-GRS-2014-0002-0011

Item 06-201: Employee management administrative records.
Disposition: Destroy when 3 years old, but longer retention is authorized if required for business use. DAA-GRS-2017-0007-0001

Item 06-203: Employee incentive award records.
Disposition: Destroy when 2 years old or 2 years after award is approved or disapproved, whichever is later, but longer retention is authorized if required for business use. DAA-GRS-2017-0007-0003

Item 06-503: Individual employee separation case files.
Disposition: Destroy 1 year after date of separation or transfer, but longer retention is authorized if required for business use. DAA-GRS-2014-0004-0003

Item 07-201: Systems and data security records.
Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/information technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

Item 07-203: System access records. Systems not requiring special accountability for access.
Disposition: Destroy when business use ceases. DAA-GRS-2013-0006-0003

Item 07-204: System access records. Systems requiring special accountability for access.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004

Item 08-102: Records management program records.
Disposition: Destroy no sooner than 6 years after the project, activity, or transaction is completed or superseded, but longer retention is authorized if needed for business use. DAA-GRS-2013-0002-0007

Item 09-202: Real property ownership records.
Disposition: Transfer to new owner after unconditional sale or Government release of conditions, restrictions, mortgages, or other liens. DAA-GRS-2016-0011-0002

Item 10-101 - Administrative records maintained in any agency office.
Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

Item 10-104: Intermediary records.
Disposition: Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. DAA-GRS-2017-0003-0002

Item 11-202: Public Correspondence and Communications not Requiring Formal Action.
Disposition: Destroy when 9

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative controls - Management oversight of activities, security awareness and training for users of the system, conduct disaster recovery exercises, separation of duties for personnel administering the system, isolating development test instances of the system. All personnel with access to the system are required to abide by the HHS and NIH Rules of Behavior upon completing security awareness training as a new hire and then annually.

Technical controls - User authentication (login) and logical access controls, anti-virus software, firewalls, role-based access through application. The database is behind a fire wall, with no direct access to it from outside the network.

Physical controls - Servers are housed in a secure climate-controlled facility with fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS). Entrances are supported with guards 24/7.