US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/03/2024

OPDIV:

NIH

Name:

NIH Google Workspace

PIA Unique Identifier:

P-9036493-155491

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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.

Google Workspace is a collection of cloud computing, productivity and collaboration tools/applications developed and marketed by Google.

NIH's instance of Google Workspace includes:
Drive,
Contacts,
Calendar,
AppSheets
Chat, and
Tasks.

Additionally, users will have access to the Google Documents (Docs) Editors suite, which include:
Docs
Sheets

Slides
Forms
Sites
Keep
AppScript

NIH disabled the use of Gmail and Meet (videoconferencing) within Google Workspace for all NIH users.

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

The type of data and information that Google Workspace will collect, maintain, and/or share include the following.

Name
Email
Phone
Date of Birth (DOB)
Mailing address
Employment status
Education records
Certificates
Device identifiers
Photographic identifiers
Financial Account Information
Medical Notes

Demographic data
Employee Records
Training records
Sensitive network and system data/information.
System vulnerability and compliance information
NIH third-party proprietary information

The following data types are considered "sensitive" and should not be collected, maintained and/or shared unless accounted for in a separate assessment.

Executable files with extensions of .exe, .jar, .dmg, .pkg, .msi, and .war
Social Security Numbers (SSN), including last 4 digits
Credit Card Numbers (CCNs)
Medical Record Number (MRN)
Grant and Contract information that is not publicly available.

Personally identifiable information (PII) and sensitive PII that is collected, maintained and/or stored outside the scope of this privacy impact assessment (PIA) is the responsibility of the NIH Institute, Center, Office (ICO) and a separate PIA must be prepared. Furthermore, sharing PII is subject to the Privacy Act and should only be disclosed in accordance with the law. Data may become PII or Sensitive PII due to context of use.

The Center for Information Technology (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.

Users log in to Google Workspace using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, including 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.

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

Google Workspace is a collection of cloud computing, productivity and collaboration tools/applications developed and marketed by Google.

NIH's instance of Google Workspace includes:
Drive,
Contacts,
Calendar,
AppSheets
Chat, and
Tasks.

Additionally, users will have access to the Google Documents (Docs) Editors suite, which include:
Docs
Sheets
Slides
Forms
Sites
Keep
AppScript

NIH disabled the use of Gmail and Meet (videoconferencing) within Google Workspace for all NIH users.

Google Workspace is built upon the Federal Risk and Authorization Management Program (FedRAMP) authorized Software as a Service (SaaS) Product Google Workspace and maintained within the Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability (STRIDES) Google Cloud Provider.

The type of data and information that Google Workspace will collect, maintain, and/or share include the following.

Name
Email
Phone
DOB
Mailing address
Employment status

Education records
Certificates
Device identifiers
Photographic identifiers
Vehicle identifiers
Financial Account Information
Medical Notes
Demographic data
Employee Records
Training records

Sensitive network and system data/information.
System vulnerability and compliance information
NIH third-party proprietary information

The following data types are considered "sensitive" and should not be collected, maintained and/or shared unless accounted for in a separate assessment.

Executable files with extensions of .exe, .jar, .dmg, .pkg, .msi, and .war
SSN, including last 4 digits
Credit Card Numbers
MRN
Grant and Contract information that is not publicly available.

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.

PII and sensitive PII that is collected, maintained and/or stored outside the scope of this PIA is the responsibility of the NIH ICO and a separate PIA must be prepared. Furthermore, sharing PII is subject to the Privacy Act and should only be disclosed in accordance with the law. Data may become PII or Sensitive PII due to context of use.

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
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers

Employment Status
Sensitive Network and data information, System Vulnerability and Compliance information, and NIH third-party proprietary information
Demographic data, Employee Records, Training Records

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, business administration and management.

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

Not Applicable

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.

09-25-0200 Clinical, Basic and Population-based Research Studies of the National Institutes of

09-25-0216 Administration: NIH Electronic Directory

OPM GOVT-1

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Email
Online
Government Sources
Within OPDIV
Other HHS OPDIV
Other Federal Entities
Non-Government Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

0925-0001 - Expiration Date: 01/31/2026
0925-0002 - Expiration Date: 01/31/2026
0925-0670 - Expiration Date: 03/31/2026
3206-0182 - Expiration Date: 08/31/2026
1615-0047 - Expiration Date: 07/31/2026

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.

Google Workspace 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 to 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 Google Workspace is used for collaboration and storage. Audit logs are be used to disclose what information is shared and tracked .

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 may 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 Google Workspace 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.

All personnel who manage or operate NIH applications must successfully complete annual security awareness training. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).

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 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 NIH Records Retention Schedules:

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

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 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 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/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

Item 03-001 - Clinical Care Services Records
These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule.
Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff. DAA-0443-2019-0001-0001

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.