US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/19/2025

OPDIV:

NIH

Name:

CIT Zoom for Government

PIA Unique Identifier:

P-3138640-138727

The subject of this PIA is which of the following?

Minor Application (child)

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Internal Flow or Collection

Describe in further detail any changes to the system that have occurred since the last PIA.

This validation is intended to refresh content. There have been no substantial changes since the last assessment. Content refresh includes the removal of employment status as a PII data element.

Describe the purpose of the system.

NIH uses Zoom for Government to conduct meetings, on-line training and other communications via telephone, web and video, with both internal and external NIH stakeholders.

Only authenticated NIH users can interact within the platform.
Individuals can present audio, share visuals on their own devices (computer, phone, tablet) and send and receive messages (chat) with audience members during live events. Sessions can be live or available on demand through recordings.

The NIH Center for Information Technology (CIT) provides assistance in supporting the Zoom for Government platform for video conferencing and collaboration and offers the meeting organizer the option of video/audio recordings of the meeting. It is the responsibility of the NIH Institute, Center, and/or Office (ICO) meeting organizer to determine whether the recorded video/audio meeting results in the development of a formal federal record.

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

NIH Users
Zoom for Government can collect, maintain, and/or share the following information retrieved from the NIH Enterprise Directory (NED), the authoritative source system:
Name
Department
Email address
Employment status (Federal employee/Direct Contractor, Guest, Tenant, Volunteer, Fellow)
NIH User ID/username (Users can choose to join as "guest" and not share their name. Their name will still be included in the meeting invite).

NIH Employees can update their information in NED via a web interface. NED maintains its own unique privacy impact assessment (PIA) with all legal authorities documented.

Non-NIH Users invited to a Zoom meeting
Zoom for Government can collect, maintain, and/or share the following information from non-NIH users invited to Zoom meetings:
Name
Email address
User ID/username (Users can choose to join as "guest" and not share their name. Their name will still be included in the meeting invite).

Customer content (audio, video, messages, files, whiteboard materials, responses to poll questions, transcriptions, responses to post-meeting or webinar feedback requests; an end user's voice or image depending on the account owner's settings.).

Users are presented with a disclaimer stating that the meeting organizer can record the meeting and it is subject to federal record guidelines. It also warns against collecting, maintaining, and/or sharing the following prohibited information:
Executable files
Social Security Numbers (SSN), including last 4 digits
Credit Card (CC) number(s)
Medical Record Numbers (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 PIA is the responsibility of the NIH ICO meeting organizer 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. Records generated with Zoom and other office automation applications must be copied by the meeting organizer to a National Archives and Records Administration (NARA) approved record-keeping system where they will be maintained for as long as they are needed by the Government and in accordance with an approved NIH or general record schedule (GRS).

Information collected by Zoom as the Cloud Service Provider (CSP) includes:
Usage Information (information about how users and devices interact with Zoom for Government)

Account Information (administrator's name and contact information, account ID, billing and transaction information, etc.).
Profile and Participant Information (display name, job information, stated locale, user ID, any other information about the end user voluntarily provided).
Device Information (Personal computer (PC) names, Media Access Control (MAC) addresses, and Internet Protocol (IP) addresses, etc.).

CIT maintains the following security safeguards:
NIH firewall protection
Multi Factor Authentication (MFA)
Security scanning and alerts using Data Loss Prevention (DLP)

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 IAM Services collects unique user credentials and stores them in an encrypted format. The IAM Services is an essential service which facilitates and governs logical access to various NIH information systems.

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

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

NIH uses Zoom for Government to conduct meetings, on-line training and other communications via telephone, web and video, with both internal and external NIH stakeholders.
Individuals can present audio, share visuals on their own devices (computer, phone, tablet) and send and receive messages (chat) with audience members during live events. Sessions can be live or available on demand through recordings.
CIT provides assistance in supporting the Zoom for Government platform for video conferencing and collaboration and offers the meeting organizer the option of video/audio recordings of the meeting. It is the responsibility of the NIH ICO meeting organizer to determine whether the recorded video/audio meeting results in the development of a formal federal record. Only authenticated NIH users can interact within the platform.
NIH Users
Zoom for Government can collect, maintain, and/or share the following information retrieved from the NED, the authoritative source system:
Name
Department
Email address
Employment status (Federal employee/Direct Contractor, Guest, Tenant, Volunteer, Fellow)
NIH User ID/username

NIH Employees can update their information in NED via a web interface. NED maintains its own unique PIA with all legal authorities documented.

Non-NIH Users invited to a Zoom meeting
Zoom for Government can collect, maintain, and/or share the following information from non-NIH users invited to Zoom meetings:
Name
Email address
User ID/username
Customer content

Users are presented with a disclaimer stating that the meeting organizer can record the meeting and it is subject to federal record guidelines. It also warns against collecting, maintaining, and/or sharing the following prohibited information:
Executable files
SSN, including last 4 digits
CC number(s)
MRN
Grant and contract information that is not publicly available

PII and sensitive PII that is collected, maintained and/or stored outside the scope of this PIA is the responsibility of the NIH ICO meeting organizer 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. Records generated with Zoom and other office automation applications must be copied by the meeting organizer to a NARA approved record-keeping system where they will be maintained for as long as they are needed by the Government and in accordance with an approved NIH or GRS.

Information collected by Zoom as the CSP includes:
Usage Information
Account Information
Profile and Participant Information
Device Information

CIT maintains the following security safeguards:
NIH firewall protection
MFA
Security scanning and alerts using DLP

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 that log in; the system uses NIH Federated Services which resides within the NIH IAM Services.

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

Yes

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

Name
Photographic Identifiers
E-Mail Address
Device Identifiers
User ID/name, Department, Profile and Participant Information, Registration Information
Data from user communications with Zoom, Account Information, Device Information, Usage Information
Customer Content, Content from Third-Party Integrations

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?

10,000-49,999

For what primary purpose is the PII used?

The names and e-mail addresses of all session participants are used to control access and to track event/session attendance.

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

Information is also used for collaborative endeavors including research, training, and general business operations.

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

44 U.S.C 3101 and 3102, Executive Order 9397, 5 U.S.C. 301 and 302, 5 U.S.C. 2105, 15 U.S.C. Chapter 63

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.

09-25-0156 Records of Participants in Programs and Respondents in Surveys Used to Evaluate

09-25-0216 Administration: NIH Electronic Directory

OPM GOVT-1, General Personnel Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

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.

There are no agreements in place that authorize information sharing or disclosure with other organizations. Since Zoom is a collaboration tool, participant's names and user IDs are voluntarily collected to allow the meeting host to track event/session attendance.

Describe the procedures for accounting for disclosures.

Audit logs are be used to disclose what information is shared and tracked. Transcripts are available for review.

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

Zoom for Government provides disclosures when individuals interact with the service that directs them to the appropriate privacy statement.

NIH personnel (employees, direct contractors, tenants, guests, Fellows and volunteers) are notified at the time of onboarding and consent to the submission and use of their personal information as a condition of employment.

All users are presented with a disclaimer, consent ,and Frequently Asked Questions (FAQ) page prior to signing on.

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.

Information is voluntarily provided. Failure to do so precludes the user from participating in Zoom sessions or trainings unless they sign in as a "Guest". Zoom tracks the IP and device information of guest accounts.

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

If Zoom for Government as the CSP makes material changes in their privacy statement, they will notify CIT Unified Unified Communications and Collaboration (UCC) of changes. CIT UCC in turn will notify users via email or user groups.

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.

Zoom for Government CSP

Individuals who believe their PII has been inappropriately obtained, used, or disclosed can contact Zoom directly through the information provided in the privacy statement.

NIH

Internal and external users of Zoom for Government who suspects their PII has been inappropriately obtained, used or disclosed may contact their NIH Privacy Coordinator and or the NIH Privacy Office at privacy@mail.nih.gov.

All NIH personnel (users) can update their PII via the NED web interface. And NIH staff can contact the NIH Service Desk if they have further concerns.

Non-NIH Users

There is no process in place for non-NIH users because they supply their username/ID whenever they accept a meeting invite and log into a meeting.

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

Zoom for Government CSP:
Zoom for Government does not periodically review the types of PII contained in the system because it only collects the minimum PII necessary to provide the services.

NIH Users
PII is not periodically reviewed for accuracy because the data is either internal, system generated data (e.g., unique identifiers) or pulled retrieved from NED. A web-based interface allows users to maintain their PII within NED.

Non-NIH Users
There is no process in place for periodic reviews of PII. PII will be reviewed by users' respective organization.

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.

NIH employs the principle of least privilege and need to know, allowing only authorized access for users which are necessary to perform primary job responsibilities in accordance with organizational missions and business functions.

Zoom for Government collects and maintains the minimum PII needed to provide the service. Users can only access PII for communications that involve them, and administrators can only access PII as necessary to provide permissions to users or monitor service usage.

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.

NIH employs the principle of least privilege and need to know, allowing only authorized access for users which are necessary to perform primary job responsibilities in accordance with organizational missions and business functions.

PII access is limited to those NIH administrators who need access to provide permissions to users, or to monitor service usage.

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 use NIH applications must complete security awareness training annually. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).

Administrators and privileged users are required to take additional training specific to their roles and responsibilities.

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

In addition to the NIH security and privacy awareness training, NIH users with contingency planning, incident response planning; and configuration management responsibilities are required to take additional training.

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 Schedule. The ICO user who sets up the meeting is responsible for retaining recordings per the NIH Record Retention/The National Archives and Records Administration (NARA) requirements.

Item # 10-010 Transitory Records
Disposition: Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule. DAA-GRS-2022-0009-
0001-

Item10-101 - Administrative records maintained in any agency office.
Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

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 12-309 - Administration: NIH Enterprise Directory (HHS/NIH)
Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

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

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

In Zoom for Government CSP
PII is secured through its use of the Amazon Web Services (AWS) GovCloud, and Zoom's internal policy limiting access to Zoom for Government PII to Federal Risk and Authorization Management Program (FedRAMP) certified individuals.

NIH
Administrative:
Authorized users are assigned particular roles, and through those role assignments acquire the system permissions to perform particular system functions. Users are assigned permissions based

on their role(s). Management of individual user rights requires assigning appropriate roles to the user's account. Users' access and corresponding permissions are reviewed once a year to assess and confirm need for continued authorized access.

Technical:
Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Physical:
Zoom for Government is a cloud based FedRAMP Software as Service (SaaS) solution. The cloud service provider, Zoom has internal policy limiting access to Zoom for Government PII to FedRAMP certified individuals.

Note: web address is a hyperlink.