US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/05/2020

OPDIV:

CDC

Name:

CDC Zoom (CDC Zoom)

PIA Unique Identifier:

P-6463043-453137

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?

No

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

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Describe the purpose of the system.

CDC Zoom is the Centers for Disease Control and Prevention implementation of the Zoom For Government Cloud based Software as a Service platform. It is a web-based video conferencing tool that allows users to meet online, with or without video, and which unifies cloud video conferencing, simple online meetings and a software-defined conference room solution into one easy-to-use platform. The solution offers video, audio, and wireless screen-sharing across various types of electronic devices and Operating Systems (OS). This tool enables CDC to bring teams and workgroups together to collaborate in a virtual environment, resulting in increased productivity and reduced costs within a secure video platform.

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

The system collects and stores: User email address and name. This information is mandatory.
The following information may also be collected as an option determined by the nature of the session: Company name and phone number; Photo/real-time video (user discretion).
In some cases, sessions may be audio recorded as well.

CDC users are authenticated via CDC Active Directory, a separate system with its own PIA. Non-CDC are authenticated by their email address that they provide to the meeting organizer and which is used to for the meeting invitation.

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

CDC Zoom uses the Federal Risk and Authorization Management Program (FedRAMP) approved solution, Zoom for Government. CDC Zoom is a web-based video conferencing tool that allows users to meet online, with or without video, and which unifies cloud video conferencing, simple online meetings and a software-defined conference room solution into one easy-to-use platform. This tool is accessible using any device and operating system; meeting participants may join virtually, from any device, boosting attendance and engagement.

The system collects and stores: Participant email address and name. This information is mandatory and is used for event access, participant identification, and event management.
The following information may also be collected as an option, determined by the nature of the session: Company name and phone number; Photo/real-time video (user discretion). This information, if provided, is also used for participant and event management.
Audio recordings of sessions may also be made and preserved for reference.

CDC users are authenticated via CDC Active Directory, a separate system with its own PIA. Non-CDC are authenticated by their email address that they provide to the meeting organizer for the meeting invitation.

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

Phone Numbers

Meeting Recordings (Voice / Video content of participants)

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose for the contact information is for access to Zoom for Government meeting sessions.

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

Recordings may be used for reference and archival purposes.

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

42 U.S.C. Sections 2 - 67

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

No

Identify the sources of PII in the system.

Email

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

No

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

Individual users of the Zoom for Government service are presented with the CDC standard System Use Notification (Warning Banner) at Log-In. The Notice reads:

"Conditions of Use and Logon:
You are accessing a US Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network., This information system is provided for US Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following:, You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system., Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose."

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.

There is no method for an individual to opt-out of the collection or use of their PII because the information is required for a user to access the Zoom service and attend the required session.

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

No changes to the data uses are anticipated. However, if there were significant changes to the system, a new PIA would be performed which would serve as notice to these individuals. Consent would be implied through the use of the tool.

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 individuals believe that their information has been compromised or inappropriately used/obtained/disclosed, they can contact the Computer Security Incident Response Team (CSIRT) via email (CSIRT@cdc.gov), or by calling 1-866-655-2245. The CSIRT works with CDC Privacy Team to resolve PII incidents and mitigate the risks associated with the inadvertent loss or unapproved disclosure of personally identifiable information (PII).

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

CDC Zoom System Administrators on a quarterly basis reviews the CDC configuration of the agency' s configuration of Zoom for Government instance to ensure the following: review account access; enabling, modifying, disabling and removing account access; and ensuring that only identified and registered CDC assigned personnel have access to the CDC Zoom instance.

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

Users:

To invite participants to hosted meeting using the individuals name/email listed in the system. The user has to be a member of a built in group to create/invite meetings.

Administrators:

Administrators create, manage, and monitor user accounts.

Contractors:

The Cloud Service Providers (CSP) are non-direct contractors and provide the hosted environment for Zoom for Government instance. The CSP has access to the the system PII and provides maintenance support for the system.

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

CDC's use of Zoom for Government leverages the built-in groups for managing the different levels of access allowed upon the system. The CDC defined User Groups within the Zoom for Government system are the following: Administrators and Standard Users. These groups are required to obtain access authorization from the CDC Zoom system stewards before being granted access.

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.

Roles within the Zoom for Government application are assigned based upon Role Based Access Controls (RBAC) and the least privilege model. The assignments correspond to the performance of their required duties which are defined to be either Users or Administrators.

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 users are required to complete annual Privacy and Security Awareness Training.

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

Users are provided training regarding the basic concepts of accessing services offered by the CDC Zoom cloud-based solution.

CDC Zoom Administrators are required to complete training in Security Incident Response, Contingency Planning and Operations, and Role-Based 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.

The General Records Schedule (GSR) 5.5, item 10 (DAA-GRS-2016-0012-0001) and item 020 (DAA-GRS-2016-0012-0002) provide the specific retention schedules.

GRS 5.5, item 10 Disposition Authority: DAA-GRS2016-00120001. Destroy when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use.

GRS 5.5, item 20 Disposition Authority: DDAA-GRS2016-00120002. Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use.

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

ADMINISTRATIVE CONTROLS:
PII is 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 CDC; completion of contractual agreements and Rules of Behavior; in accordance with applicable CDC policies.

TECHNICAL CONTROLS:
Technical controls applied to CDC Zoom include: continuous network/system monitoring; FIPS 140-2 compliant encryption of data in transit; firewalls; and authentication where applicable.

PHYSICAL CONTROLS:
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; and, 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. 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; and, 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.

Identify the publicly-available URL:

https://cdc.zoomgov.com/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No