

Date Signed: 7/1/2022

Acronyms

ATO - Authorization to Operate
 CAC - Common Access Card
 FISMA - Federal Information Security Management Act
 ISA - Information Sharing Agreement
 HHS - Department of Health and Human Services
 MOU - Memorandum of Understanding
 NARA - National Archives and Record Administration
 OMB - Office of Management and Budget
 PIA - Privacy Impact Assessment
 PII - Personally Identifiable Information
 POC - Point of Contact
 PTA - Privacy Threshold Assessment
 SORN - System of Records Notice
 SSN - Social Security Number
 URL - Uniform Resource Locator

General Information

Status:	Approved	PIA ID:	1456158
PIA Name:	FDA - OC FDA Zoom - QTR2 - 2022 - FDA2060697	Title:	FDA - OC FDA Zoom
OpDiv:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Contractor
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	10/21/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	Zoom is a secure web-based communication application that supports the need for information sharing and collaboration. It

provides FDA's user community the ability to interact with internal and external participants in order to conduct and facilitate meeting via telephony, web, and video. FDA uses Zoom to conduct online training, meetings, and other communications. Presenters can share visuals of their own device (e.g., laptop computer), desktops or of documents (most often PowerPoint or similar software documents), present audio, and send and receive messages with audience members (attendees during live events). These sessions can be live or on demand.

Zoom also has the capability to record meetings/sessions (audio and/or video) if the host chooses to record the event.

The users of Zoom include FDA employees and Direct Contractors, approved third-party contractors who help maintain the system and at times, other federal, state and local employees and/or members of the general public may attend events held via Zoom.

PTA - 9:

List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.

Zoom collects the following personally identifiable information (PII): (a) first and last name; (b) email address; (c) phone number; (d)

biometric and photographic (voice, face) identifiers if the meeting is recorded; (e) account username and password; and (f) any other PII that users choose to share or disclose in a recorded Zoom session. FDA retains the PII for as long as the individual has a Zoom account. The PII is not shared with any other system or organization.

Zoom also collects non-PII relevant to a particular event/session, e.g., the content of a set of slides about a given topic.

Zoom is used to manage event registrations. Event registrations require a username and password which is unique to each specific Zoom event. These event registration passwords are masked and not stored in the system. If a user is locked out of the system, a link to reset a Zoom user's password can be provided upon the user's submission of a request via the email address that is collected by the system. No separate systems are used for credential handling or storage.

Content is accessed via a landing page on the internet. Access credentials (username and password) are required to access the content. Users are provided an initial password which they may then change.

All passwords are masked within the system with the exception of the passwords for the meetings themselves. Stored passwords are masked and unviewable, even to the Administrator.

PTA -9A: Are user credentials used to access the system?

Yes

PTA - 10: Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual

Zoom is hosted in a cloud-based FedRAMP approved environment, Software-as-a-Service (SaaS). FDA utilizes the system to collaborate

with individuals and groups, including conducting meetings, webinars, and events requiring closed captioning.

Zoom allows FDA users (employees, Direct Contractors, and third-party contractors such as vendor support provided by Verizon and Cisco) and Business Partners/Contacts (Federal, state, local agencies) to communicate in virtual meetings.

FDA personnel who use Zoom does not use any personal identifiers to retrieve records held in the system.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	<p>Name</p> <p>E-Mail Address</p> <p>Phone numbers</p> <p>Photographic Identifiers</p> <p>Biometric Identifiers</p> <p>Others - username and password; Biometric identifiers and photographic image refer to voice and facial image</p>
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	<p>Business Partners/Contacts (Federal, state, local agencies)</p> <p>Employees/ HHS Direct Contractors</p> <p>Public Citizens</p> <p>Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)</p>
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	201 - 500
PIA - 4:	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. The usernames and passwords are used to authenticate into a Zoom session.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	The implementation of this system is authorized by 5 U.S.C. 301. This statute empowers agency

		<p>heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures of the system are required by the Federal Information Security Modernization Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.</p>
<p>PIA - 9:</p>	<p>Identify the sources of PII in the system</p>	<p>Directly from an individual about whom the information pertains</p> <ul style="list-style-type: none"> In-person Online <p>Government Sources</p> <ul style="list-style-type: none"> Within the OPDIV Other HHS OPDIV Other Federal Entities <p>Non-Government Sources</p> <ul style="list-style-type: none"> Members of the Public Public Media/Internet Private Sector
<p>PIA - 10:</p>	<p>Is the PII shared with other organizations outside the system's Operating Division?</p>	<p>No</p>
<p>PIA - 11:</p>	<p>Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason</p>	<p>After users enter their credentials to attend a meeting or watch a recorded presentation, they receive a pop-up screen with a privacy notice. This is true for both FDA and non-FDA Computer systems accessing Zoom.</p> <p>FDA personnel (employees and Direct Contractors) are also notified at the time of hire and consent to the submission and use of their personal information as a condition of employment.</p> <p>FDA Privacy and website policies are posted on all FDA.gov and FDA intranet pages. This PIA provides further notice.</p>
<p>PIA - 12:</p>	<p>Is the submission of PII by individuals voluntary or mandatory?</p>	<p>Voluntary</p>
<p>PIA - 13:</p>	<p>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</p>	<p>Individuals are not required by law to provide PII and will not suffer a criminal or civil penalty</p>

		<p>should they opt not to provide their PII. As a practical matter, FDA employees are often required to provide PII because the FDA meeting organizers may need to track attendance or for controlling access to meetings. FDA personnel may also opt to sign in as guests (not disclose their name) depending on the requirements set by the Host or by applicable policies. Members of the public may be invited to attend meetings and can sign in as guests.</p>
<p>PIA - 14:</p>	<p>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). Alternatively, describe why they cannot be notified or have their consent obtained</p>	<p>If a major change occurs, the agency will notify individuals whose PII is in the system by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice, amended pop-up language, information provided at new employee orientation, or informal processes such as e-mail notice to the individuals.</p>
<p>PIA - 15:</p>	<p>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</p>	<p>Internal and external users of Zoom who suspect their PII has been inappropriately obtained, used or disclosed in have a number of options available to resolve the situation regarding their PII. The users may contact the FDA via email, phone and standard mail avenues (all listed on fda.gov). Specific offices that individuals may contact include FDA's Privacy Office.</p> <p>FDA employees may also contact the Employee Resources and Information Center (ERIC) or the Systems Management Center (SMC) to seek assistance with concerns about PII including use, collection, theft, and to correct any inaccurate PII.</p>
<p>PIA - 16:</p>	<p>Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not</p>	<p>PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. Accuracy is ensured by individual</p>

review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by privacy and security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. OC FDA Zoom administrators perform annual reviews to evaluate user access.

PII relevancy is supported by policy (HHS Rules of Behavior, need-to-know restrictions and others) and by design of fields and content that solicit only relevant and necessary PII.

Systems authorization, testing and continuous monitoring ensure technical integrity, availability and accuracy of data.

The integrity, availability, accuracy and relevancy of PII about agency personnel is also supported by similar and/or additional measures applied at the source system level.

Administrators also randomly check all Zoom user accounts to spot potential problems (integrity, availability, accuracy) and the hosting provider monitors the Zoom system to check for bugs. In the event that a Zoom account has been inactive for 60 days, it will automatically be deactivated.

Personnel wishing to correct inaccurate or out of date information may do so by contacting an administrator or updating it themselves if they possess account access.

Public citizens who opt to provide their contact information are responsible for providing accurate information and may independently update and correct their information at any time. Information related to external submitters is corrected in the course of use and/or at the request of the individual.

<p>PIA - 17:</p>	<p>Identify who will have access to the PII in the system and the reason why they require access</p>	<p>Users Administrators Developers Contractors</p>
<p>PIA - 17A:</p>	<p>Provide the reason of access for each of the groups identified in PIA -17</p> <p>Users: Meeting attendees have access to names as they appear on attendee rosters.</p> <p>Administrators: Administrators have access to PII in order to grant access to the system for those who wish to host Zoom meetings. Some of the administrators are direct contractors.</p> <p>Developers: developers have access to PII while providing operations and maintenance support, developing patches, updates, troubleshooting support.</p> <p>Contractors: The Direct Contractors possess administrative access to perform operations and maintenance support, as well as troubleshoot user issues.</p>	
<p>PIA - 17B:</p>	<p>Select the type of contractor</p>	<p>HHS/OpDiv Direct Contractor</p>
<p>PIA - 18:</p>	<p>Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII</p>	<p>Presentation attendees who require access to the information system need to obtain meeting organizer authorization before access is granted. The agency reviews the access list for the system randomly to review and adjust access permissions for content creators, and, to remove unnecessary accounts from the system through the User Access Review. The determination regarding who may access the PII in the system is made by a system administrator and validated through the process above.</p>
<p>PIA - 19:</p>	<p>Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job</p>	<p>Event hosts use technical methods and controls to limit access to PII to the minimum necessary to accomplish authorized functions and to that which is relevant to the meeting or other event being conducted via Zoom. These methods include use of Zoom settings and options, host sharing or not sharing control of the event display and audio, and the host's control over whether to require and subsequently display attendee email addresses during the event and in any recordings.</p>
<p>PIA - 20:</p>	<p>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</p>	<p>All system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating</p>

to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that individuals successfully complete the training.

PIA - 23:

Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)

Because the personnel data stored in the systems databases are copies of data pulled from other sources, they are temporary records in accordance with National Archives and Records Administration (NARA) DAA-GRS-2017-0007-0001. As such, they are destroyed when the business use ceases. Specifically, when updated with new data, the system deletes old data for which there is no longer a business use.

In accordance with DAA-GRS-2013-0006-0003, user account information and logs are destroyed when their business use ceases.

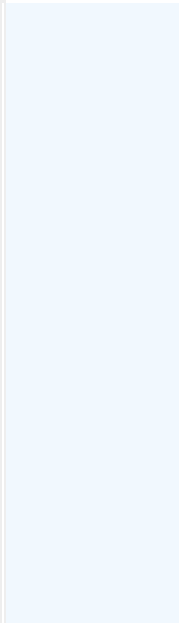
The user account records for Zoom are maintained in accordance with DAA-General Records Schedule (GRS)-2013-0006-0003 with the logs being destroyed when business use ceases.

Any audio or video files created in Zoom are maintained under GRS 3.2 item 010. The disposition authority is DAA-GRS-2013-0006-0001, and the records are destroyed 1 year after they are no longer needed for Agency or IT administrative purposes.

PIA - 24:

Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response

Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and



Minimum Necessary principles when awarding access, and others.

Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools.

Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls.

Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.