Privacy Impact Assessment (PIA): FDA - Adobe Connect - QTR2 - 2022 - FDA2041950

Date Signed: 4/27/2022

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:**	1440808
PIA Name:	FDA - Adobe Connect - QTR2 - 2022 - FDA2041950	**Title:**	FDA - OC Adobe Connect
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?	Yes

URL Details

Type of URL	List Of URL
Internet (publicly available)	https://collaboration.fda.gov

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	4/20/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	Since the last privacy assessment, Adobe Connect has been upgraded from version 9 to version 11. This update took place in November 2020 and the primary changes were to make the system HTML 5 compliant and no longer reliant upon Flash. This change does not affect any of the responses in this PIA.
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?	The purpose of the Office of the Commissioner (OC) Adobe Connect system (System or the System) is to collaborate

		virtually for training or mission critical purposes. The Food and Drug Administration (FDA) uses this System to conduct virtual collaborative training (both asynchronous and synchronous); host large-scale public meetings or webinars and to extract training metrics in order to improve future trainings. This system does not receive or send information to any other systems.
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.	The System collects the following PII information: (a) first and last name; (b) work email address; and (c) biometric identifiers. The PII data is not shared with any other system or

		organization. The System also collects the following non-PII data: (a) entire recordings of meetings (audio and/or video) or events if the host chooses to record them; (b) records of meeting attendance and completions; and, (c) data relevant to a particular session. (e.g., the content of a set of training slides about a given topic.) The users of the System include FDA employees (any role listed below), FDA Direct Contractors (any role listed below), and the general public (participants). Only FDA employees and FDA Direct Contractors have the ability to obtain accounts with login credentials. User access to Adobe Connect is limited in duration to that time period for which the user requires access and/or is employed by the FDA. The System provides role-based access that includes the following 5 major roles: Administrator; Host; Presenter; Learner; and Participant. Administrators are granted full access to information stored in the System. The number of Administrators is limited to a few Federal employees and contractors who maintain the system. "Hosts" can host meetings and events and only have access to the information surrounding their specific events. Hosts are FDA employees and Direct Contractors. Each host controls presenter and user access for the specific meeting or event for which he or she is host. Presenters (e.g., speaker, teacher) can present content such as PowerPoint presentations, audio, video, or combinations thereof. "Learners" attend training and educational events provided via Adobe Connect. They can sign up for training events that are available in the system, and utilize a username and password to access the training. "Participants" can attend meetings and events that they are given access to, usually through a web link/URL. They can attend as a guest or if necessary, sign up and register for the event by providing a username and password that only work to access that specific event. Users with account credentials receive their accounts from existing system Administrators. When an FDA employee or Direct Contractor requests an account, the Administrator validates the need for access and establishes an account using the FDA email address of the requestor. Appropriate roles are set according to the needs of the individual and the agency. Once the account is established, a temporary password is sent to the user who then resets their password to one of their choice that follows FDA password policies.
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	Adobe Connect is hosted in a cloud-based FedRAMP approved environment managed and owned by an entity known as the Committee of Sponsoring Organizations (CoSo).

	about each category of individual	CoSo provides both Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) support. Adobe Connect sits in the CoSo environment as a Software-as-a-Service (SaaS) based solution that is managed and owned by the FDA. The FDA utilizes the system to collaborate with individuals and groups to conduct meetings and learning events such as online training, webinars, and events requiring closed captioning. FDA personnel who access or use the system do not use any personal identifiers to retrieve records held in the system. Users enter user access credentials to access a session, however user access credentials are not stored in the Adobe Connect system. Users obtain credentials upon request by providing an FDA email address and a justification for the account and required level of access. Users set their own passwords. These authentication credentials are stored separately within the FedRAMP environment and passwords are masked. Adobe Connect collects the following PII: first and last name, work email address (which is also made to be the username), biometric identifiers, and there is an optional field for "HHS ID." The credentials are collected and maintained within the Adobe Connect system. Adobe Connect hosts determine who has access to content. Hosts upload training or documents for meetings and learning events and they determine what PII is contained in the content that they upload. Hosts create courses that use recorded content and live training. Additionally, hosts create and manage the meetings and determine access to content. In some cases, FDA personnel and/or members of the public have access to first and last names of meeting attendees that are visible during the meeting or event. However, only administrators have access to account holder's username and HHS ID. The PII data is retained as long as the training containing the PII is still relevant. Administrators' ability to retrieve system records is limited to retrieval by unique meeting number. Administrators have access to the full inventory of meetings created, and one data field contains the Host's name, but (a) there is no way to use this data element as a search term, and (b) this is never done in practice because it would be inefficient and unlikely to be necessary.
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	Name E-Mail Address Biometric Identifiers Others - HHS ID number for FDA/HHS personnel located on the back of the FDA HSPD-12 badge; and (b) User access credentials such as username and password for account creation. Note: Hosts control whether their recorded materials contain PII. Any other PII users wish to share in use of Adobe Connect.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Public Citizens Other
PIA - 4:	For what primary purpose is the PII used?	The names and email addresses of all participants are used to control access and to track attendance during training and meetings/webcasts, as well as notify attendees of future meetings. HHS IDs for FDA personnel are used to report course completion to the HHS Learning Management System (LMS). The LMS PIA can be found on the HHS website.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	None
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	Authorities: 21 U.S.C. 379 and 5 U.S.C. 301. FDA conducts training as required under the Food, Drug and Cosmetic Act at 21 U.S.C. 379l(a), which states, "In general... The Secretary shall conduct training and education programs for the employees of the Food and Drug Administration relating to the regulatory responsibilities and policies established by this chapter, including programs for— (1) scientific training; (2) training to improve the skill of officers and employees authorized to conduct inspections under section 374 of this title; (3) training to achieve product specialization in such inspections; and (4) training in administrative process and procedure and integrity issues."
PIA - 8:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	This is not a Privacy Act System.
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Non-Government Sources

		Members of the Public Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	The collection is not subject to the Paperwork Reduction Act.
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	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 Adobe Connect. FDA personnel (employees and Direct Contractors) are notified at the time of hire and consent to the submission and use of their personal information as a condition of employment. Information about the collection and use of information is provided during new employee orientation and training as well as within the system's user manuals and training. FDA center representatives, and the various individuals involved with the specific data collection and use provide notification to the employees and non-employees at the time the data is requested. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet (https://www.fda.gov/about-fda/about-website/website-policies) pages. This PIA provides further notice.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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	Individuals are not required by law to provide PII and will not suffer a criminal or civil penalty 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 and course creators may need to track attendance of training taken and course completion or for controlling access to meetings. Members of the public may be invited to attend meetings and/or trainings and can sign in as guests. Meeting organizers can permit attendees to effectively opt-out of providing PII by signing in using “guest access”, which allows attendees to view materials without submitting PII. Meeting organizers may choose whether to permit guest access to a given presentation.
PIA - 14:	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	If FDA changes its practices with regard to the collection or handling of PII related to the website, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include email to individuals, adding or updating online notices or forms, or other available means to inform the

		individual.
PIA - 15:	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	Users of Adobe Connect 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. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone and standard mail avenues (all listed on FDA.gov and the FDA intranet). Public citizens may use many different methods to raise concerns, including contacting FDA offices through FDA.gov (phone, mail, email). HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all reports of suspected breaches must be reported to the CIOCC.
PIA - 16:	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	Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. Accuracy is ensured by individual 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. PII relevancy is supported through the design of the system to require and collect only the PII elements necessary to administer the system and enable its intended use. 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. Office of the Commissioner (OC) performs quarterly reviews to evaluate user access.

PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Contractors Others
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17	Users: Meeting and training attendees have access to names as they appear on attendee rosters. Attendees and members of the public do not normally have access to email addresses. They can have access to email addresses if Adobe Connect content creators, course developers need to track attendance of training taken and course completion or for controlling access to meetings. Administrators: The FDA Adobe Connect System Administrators have access to all PII within the system because they control access to Adobe Connect. They have access to content creators that have received credentials to create content using the system. Some Administrators are Direct Contractors. Contractors: The FDA Adobe Connect System Administrators have access to all PII within the system because they control access to Adobe Connect. They have access to content creators that have received credentials to create content using the system. Some Administrators are Direct Contractors. Others: Adobe Connect hosts (FDA employees, Direct Contractors, and third-party contractors) have access to names and email addresses to control and track attendance. The FDA Adobe Connect System Administrators have access to all PII within the system because they control access to Adobe Connect. They have access to content creators that have received credentials to create content using the system. Some Administrators are Direct Contractors.
PIA - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	Course and presentation attendees who require access to the information system need to obtain meeting organizer and Center IT Liaison approval and sign off 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.
PIA - 19:	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	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 Adobe Connect. These methods include use of Adobe Connect 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.
PIA - 20:	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 system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating 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 Digital Transformation (ODT) verifies that individuals successfully complete the training.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	System administrators complete the FDA systems administrator training course prior to receiving access. Updates are provided as new information or features are released. If there are any major changes made that require additional training, the Adobe Training officer will ensure all Adobe users will receive the requisite training. Additional role-based training on privacy is available via FDA's privacy office.
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 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. Audio and video records created by Adobe Connect to memorialize meetings are treated as official records under File Code 8420, Program Management Files. General Records Schedule (GRS) 3.2 Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. 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.
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.
PIA - 25:	Describe the purpose of the web site, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response	This website is for users who have credentials to log in and set up meetings or events.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	Yes
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	Session Cookies - Does Not Collect PII
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No