



Privacy Impact Assessment

For
NCRTM Webinar Platform – Adobe Connect 9

Date:

May 30, 2014

Point of Contact:

Kristen Rhinehart-Fernandez
Kristen.Rhinehart@ed.gov

System Owner:

RoseAnn Ashby
Chief, Training Programs Unit
RoseAnn.Ashby@ed.gov

(Please note: The Webinar Platform is operated through a contract with New Editions.
Cherie Takemoto is the Project Manager at: ctakemoto@neweditions.net)

Author:

Kristen Rhinehart-Fernandez

**Office of Special Education and Rehabilitative Services (OSERS)
Rehabilitation Services Administration (RSA)**

U.S. Department of Education



1. System Information.

Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

NCRTM Webinar Platform - Adobe Connect 9 is a web conferencing application that brings multiple parties together by providing virtual conference rooms where parties can enter to see online presentations, share documents, and provide other multimedia online content while simultaneously discussing said content over a shared phone conference line. The product works seamlessly for anyone who has common desktop software including a web browser and Adobe Flash® Plugin. Since Adobe Flash® is installed on virtually all existing desktops, Adobe Connect 9 effectively requires no additional client software to operate.

The primary purpose is to conduct web-based technical assistance in the form of interactive webinars. We anticipate conducting 15 webinars during the base period (May 1, 2014-December 1, 2014) and 25 webinars in the option period (December 1, 2014-September 30, 2015). The length of time will not exceed 1.5 hours. Each webinar will have no more than 200 participants.

2. Legal Authority.

Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The system is authorized by section 13 of the Rehabilitation Act of 1973 (the Act), as amended. Section 10 of the Act permits the Commissioner authority to administer these programs effectively and efficiently. Section 302 of the Act authorizes the Rehabilitation Training program and these program funds are being used to support this contract.

3. Characterization of the Information.

What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

No sensitive PII is collected. The elements to be collected are:

- First and last name
- Title
- Organization
- Work email address
- Requests for accessibility accommodations that go beyond accessible digital files and,
- Open captioning which is automatically provided for each webinar (voluntary)

The sources of the information are from the individual registering for the webinar.

The information will be collected online through a webinar registration form. The registration information, classroom chat information, and training content will be removed from the site after each



webinar. The recorded webinars will be stored on the NCRTM repository, not on the Adobe Connect system.

This information is not used to link or cross-reference multiple databases.

4. Why is the information collected?

How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The purpose for collecting this information is to: 1) confirm the number of attendees and types of entities represented, 2) confirm attendee name if the webinar is a required grant activity, 3) ensure that all participants are able to successfully log onto the webinar and fully participate, 4) disseminate webinar materials such as the recording, transcript, PowerPoint slides, and other supporting documentation, and 5) using a standard evaluation instrument, identify the quality, relevance, and usefulness of the webinar and how participants plan to implement the knowledge, skills, and abilities gained in order to change behavior and or practice.

5. Social Security Number (SSN).

If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

SSNs will not be collected.

6. Uses of the Information.

What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

Internal and/or external uses of the information: 1) confirms the number of attendees and types of entities represented, 2) confirms the number of attendees if the webinar is a required grant activity, 3) ensures that all participants are able to successfully log onto the webinar and fully participate, 4) disseminates webinar materials such as the recording, transcript, PowerPoint slides, and other supporting documentation, and 5) using a standard evaluation instrument, identifies the quality, relevance, and usefulness of the webinar and how participants plan to implement the knowledge, skills, and abilities gained in order to change behavior and or practice.

There are no additional types of methods used to analyze the data.

The system does not use commercial information, publicly available information, or information from other Federal agency databases.



7. Internal Sharing and Disclosure.

With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

The information will only be used by RSA and not shared with other Department of Ed components.

8. External Sharing and Disclosure.

With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

The information will not be shared with any external entities.

9. Notice.

Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Notice is provided to the individuals prior to collection of their information. The following notice is prominently placed on the website where the information is collected.

“By registering for this Webinar, you are agreeing to provide information necessary to conduct the RSA Webinars and distribute information.”

The name used to sign onto the webinar may be viewable on the participant chat screen during the webinar. Other personal data gathered by the NCRTM Webinar system is restricted to authorized staff.

Information collected is not transferred to third parties.

10. Web Addresses.

List the web addresses (known or planned) that have a Privacy Notice.

URLs are generated as the webinar is created so they are different for each event. Following is a registration link and an info link. The bold portion changes with each event:

<https://neweditions.adobeconnect.com/e2gb46oqxx2/event/registration.html>



11. Security.

What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

The required network traffic of the service is protected by SSL encryption. The internal system register is protected by personal user accounts, and by personal authorization of the system administrators.

The data center is SSAE 16 certified and security controls are in place including strong doors with locks, video monitoring, physical access logs, and secured windows.

- The data centers are in well-constructed, physically secured buildings
- The hosted environment is broken into clusters which are operationally identical and thus provide good failover and redundancy
- Existing backup facilities are physically and logically separated from production systems
- The data centers used have good power backup through the use of backup generators and occasionally connections to multiple power grids
- The data centers have good fire suppression capabilities throughout each facility

Adobe maintains good change management and change control practices for its hosted environment which include:

- Document control
- Change management systems
- Backup restoration
- Incident response capability (in partnership with ASSET)
- Compliance Controls

Adobe Connect 9 has a good breadth of features to enable various compliance controls within the application. Although too numerous to mention individually, some of the key features include:

- Type based content restrictions via content 'pods' which can be enabled and disabled per meeting
- Meeting recordings and detailed logs. Meetings can be recorded for both video and audio. This is important for compliance with various regulations in different jurisdictions
- Controlled access to meetings

Adobe Connect 9 had a good suite of security features for protecting customer communications and information. The features could be broadly viewed as falling into one of these following categories:

- User authentication – including password management
- Authorization – including enforcement of XML API security levels and ACLs, as well as configurable user security levels and permissions
- Auditing and logging – including a configurable application logging function



A security assessment was conducted by Securisea, an independent information security company specializing in Financial Services, Education, Healthcare, Manufacturing, Media, Retail, Software/ISV, and Telecom/ISP.

12. Privacy Act System of Records.

Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

A system of record notice (SORN) is not needed because the information collected is not retrieved by any personal identifiers. Therefore, a system of record as defined by the Privacy Act is not being created, and the reporting requirements of OMB Circular A-130 do not apply.

13. Records Retention and Disposition.

Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

NCRTM manages records in accordance with NARA's General Records Schedule 20 (<http://www.archives.gov/records-mgmt/grs/>) and: "Grant Administration and Management Files," Schedule Locator 254. The NARA disposition authority is N1-441-11-001.