

**Privacy Impact Assessment (PIA)**

for the

National Clearinghouse for Rehabilitation Training Materials (NCRTM)

**Jun. 7, 19**

**For PIA Certification Updates Only:** This PIA was reviewed on June 7, 2019 by **Kristen Rhinehart-Fernandez** certifying the information contained here is valid and up to date.

**Contact Point**

**Contact Person/Title: Kristen Rhinehart-Fernandez**

**Contact Email: Kristen.Rhinehart@ed.gov**

**System Owner**

**Name/Title: Kristen Rhinehart-Fernandez**

**Principal Office: Office of Special Education Rehabilitative Services (OSERS)**

**Please submit completed Privacy Impact Assessments to the Privacy Office at** [**privacysafeguards@ed.gov**](mailto:privacysafeguards@ed.gov)

*Please complete this* ***Privacy Impact Assessment (PIA)*** *on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*

***If a question does not apply to your system, please answer with N/A.***

# Introduction

* 1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The system contains the National Clearinghouse for Rehabilitation Training Materials (NCRTM). The NCRTM is the centralized repository for the collection, dissemination, and utilization of training and technical assistance materials. RSA-funded discretionary grantees are required to submit all materials developed with grant funds to the NCRTM. This grant requirement is contained in all application packages. Grantees may include but are not limited State and public or nonprofit agencies and organizations, including American Indian tribes and institutions of higher education. Other vocational rehabilitation professionals may also post materials for RSA to consider including in the NCRTM. The materials submitted to NCRTM inform the field of vocational rehabilitation and may be used to identify emerging and promising practices, as well as data and information describing issues, challenges, and trends in the field. Additionally, it contains examples of materials used to effectively train and prepare vocational rehabilitation counselors and professionals for today’s marketplace.

* 1. Describe the purpose for which the personally identifiable information (PII)[[1]](#footnote-1) is collected, used, maintained or shared.

The source of the content is from rehabilitation professionals who submit materials – they or their organizations develop - for RSA to consider including in the NCRTM. They are primarily RSA grantees. The NCRTM librarian (a system administrator) uses the information collected to contact individuals if there are questions about or issues with the materials they have submitted.

* 1. Is this a new system, or one that is currently in operation?  
     Currently Operating System
  2. Is this PIA new, or is it updating a previous version?  
     Updated PIA
  3. Is the system operated by the agency or by a contractor?

Contractor

* + 1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

Yes

# Legal Authorities and Other Requirements *If you are unsure of your legal authority, please contact your program attorney.*

* 1. Whatspecific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

Legislative Authority: Section 15 of the Rehabilitation Act of 1973 (Rehabilitation Act), as amended by the Workforce Innovation and Opportunity Act (WIOA). SEC. 15. (a) The Secretary of Education shall establish a central clearinghouse for information and resource availability for individuals with disabilities which shall provide information and data. The clearinghouse shall also provide any other relevant information and data which the Secretary of Education considers appropriate. (b) The Commissioner may assist the Secretary of Education to develop within the Department of Education a coordinated system of information and data retrieval, which will have the capacity and responsibility to provide information regarding the information and data referred to in subsection (a) of this section to the Congress, public and private agencies and organizations, individuals with disabilities and their families, professionals in fields serving such individuals, and the general public. (c) The office established to carry out the provisions of this section shall be known as the ‘‘Office of Information and Resources for Individuals with Disabilities’’. (d) There are authorized to be appropriated to carry out this section such sums as may be necessary. [29 U.S.C. 712]

**SORN**

* 1. Is the information in this system retrieved by an individual’s name or personal identifier such as a Social Security Number or other identification?   
       
     No  
     1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[[2]](#footnote-2) Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.



Click here to enter text.

* + 1. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.   
       

The information is not retrieved by an identifier.

**Records Management**

**If you do not know your records schedule, please consult with your records liaison or send an email to** [**RMHelp@ed.gov**](mailto:RMHelp@ed.gov)

* 1. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

NCRTM manages records in accordance with the Department: <https://www2.ed.gov/notices/records-management/index.html> (schedule locator number 254: Grant administration and management files, disposition

N1-441-11-001**)**, **section E final grant products**, **routine products and products determined to be of “historical significance”.** The NCRTM is the only repository that exists in the Vocational Rehabilitation field. Products on the NCRTM are submitted by grantees and the field for informational purposes or to fulfill grant performance requirements which are of enduring value. In accordance with the Statute that mandates the NCRTM, products contained on the NCRTM are to be retained permanently. The program office will determine if there are any products that are out of date or no longer relevant due to changes in the law or program regulations and will remove those products from the NCRTM, as necessary.

* 1. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Yes. If products are determine to be no longer relevant, they will be removed from the NCRTM.

# Characterization and Use of Information

**Collection**

* 1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The following information is collected (\* indicate required fields):

* Name\*
* Job Title\*
* Organization\*
* Organization Website
* Work email address\*
* Work Phone number\*
* Address, City, State, Zip
* RSA PR/Award Number
  1. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

* 1. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

Vocational rehabilitation professionals, primarily RSA grantees (i.e., representatives from State and public or nonprofit agencies and organizations, including American Indian tribes and institutions of higher education.) are the sources of the information collected.

* 1. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The information is collected via web forms – for either individuals who submit materials to the NCRTM for RSA’s consideration or for individuals who register for webinars.

* 1. How is the PII validated or confirmed to ensure the integrity of the information collected?[[3]](#footnote-3) Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The information is validated using an automated process to confirm the data entered meets specific requirements:

* Name\* – Text.
* Job Title\* – Text.
* Organization\* – Alphanumeric.
* Organization Website – includes http:// or https:// in the URL.
* Work email address\* – includes @.com, @.net, etc.
* Work Phone number\* – ###-###-#### format.
* Address, City, State, Zip – Zip in ##### format.
* RSA PR/Award Number – HnnnAnnnnnn where A is any letter and n is any digit.

**Use**

* 1. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The NCRTM librarian (a system administrator) uses the information to follow up with individuals if there is a question about their submissions - for example, if the material is not accessible to people with disabilities, if they forgot to attach a file (i.e., the material), forgot to add topics for indexing in the library, etc. The information is also used to create accounts if the individuals desire. Accounts do not require individuals to submit the information each time they submit a material, allowing them a simple convenience if they plan to post multiple materials. The account also allows them to view whether materials they have previously submitted have been approved or denied by RSA for inclusion in the NCRTM.

* 1. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?   
       
     No  
     1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?  
        

Click here to enter text.

**Social Security Numbers**

*It is the Department’s Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

* 1. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

* + 1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.   
       

Click here to enter text.

* + 1. Specify any alternatives considered in the collection of SNNs and why the alternatives were not selected.  
       

Click here to enter text.

# Notice

* 1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Notice is provided to the individuals on the submission and NCRTM registration pages prior to collection of the PII.

* 1. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.  
     

The following statement is located on NCRTM’s Login (<https://ncrtm.ed.gov/Account/Login.aspx>) and Registration (<https://ncrtm.ed.gov/Account/Register.aspx>) pages:

The purpose of the NCRTM member portal is for RSA grantees to upload documents funded by RSA, and for organizations/individuals to submit multiple materials. When a grantee creates an account, materials uploaded will be directed to the responsible RSA project officer for review per RSA grantee requirements. Members who have created an NCRTM account can check on the status of a submitted material or upload new materials to the NCRTM.

* 1. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Individuals may affirmatively request to join a webinar or submit materials as aforementioned. They can contact NCRTM if they do not wish to complete a form and still attend a webinar or submit materials and bypass providing the information.

* 1. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

# Information Sharing and Disclosures

**Internal**

* 1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.  
       
     No
  2. What PII will be shared and with whom?  
     

Click here to enter text.

* 1. What is the purpose for sharing the specified PII with the specified internal organizations?   
     

Click here to enter text.

**External**

* 1. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.  
       
     No
  2. What PII will be shared and with whom? List programmatic disclosures only.[[4]](#footnote-4)   
     **Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.   
     

Click here to enter text.

* 1. What is the purpose for sharing the PII with the specified external entities?  
     

Click here to enter text.

* 1. Is the sharing with the external entities authorized?  
     

Click here to select.

* 1. Is the system able to provide and retain an account of any disclosures made and make it available upon request?  
     

No

* 1. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?  
     

Click here to enter text.

* 1. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?  
     

Click here to select.

* 1. Does the project place limitation on re-disclosure?  
       
     Click here to select.

# Redress

* 1. What are the procedures that allow individuals to access their own information?

The individual can email NCRTM librarian at NCRTM@neweditions.net.

* 1. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The individual can email NCRTM librarian at NCRTM@neweditions.net.

* 1. How does the project notify individuals about the procedures for correcting their information?

The NCRTM email is presented on the Contact Us page of the website.

# Safeguards *If you are unsure which safeguards will apply, please consult with your* [*ISSO*](https://share.ed.gov/teams/OCIO/IA/SEA/SEA_Collab/SitePages/ED%20ISSOs.aspx)*.*

* 1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

* 1. Is an Authority to Operate (ATO) required?  
       
     Yes
  2. Under [NIST FIPS Pub. 199](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf), what is the security categorization of the system: **Low, Moderate, or High?**  
     Low
  3. What administrative, technical, and physical safeguards are in place to protect the information?

New Editions Consulting, Inc maintains and Microsoft Azure houses the NCRTM for ED. New Editions Physical and Environmental Protection Policy and Procedure is a formal document that outlines the policies, procedures, and protocols for physical and environmental protection of New Editions-owned and -supported information systems and the PII contained within them. Protections include: video monitored reception area; a visitor log; elevator keys to access the floor office during non-business hours; requirement that users log off their computers when they are not at their desks; etc. These safeguards help to prohibit unauthorized individuals from gaining access to the system and the information contained within it while at the New Editions office.

Microsoft Azure enforces physical access authorizations for all physical access points to Azure datacenters using 24x7 staffing, alarms, video surveillance, multifactor authentication, and man-trap portal devices. Physical access to a Microsoft Azure datacenter must be approved by the Datacenter Management (DCM) team using its datacenter access tool. Access levels are assigned in the tool to either a user’s Microsoft issued badge or a temporary access badge that is assigned at the datacenter by the Control Room Supervisor (CRS). Access levels are approved by the DCM team. In addition to credentials assigned to physical badges, some areas of the datacenter require enrollment of the user’s biometric data (hand geometry or fingerprint). Additionally, when access is no longer required, datacenter security officers or management manually request the termination of access.

Additionally, annually, and as warranted, staff who have access to the NCRTM application are provided security and privacy awareness and protecting information training. The training includes information on what constitutes PII and Sensitive PII (SPII) and how to maintain, protect, and safeguard it, as well as the steps to perform if PII/SPII is unlawfully accessed.

* 1. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

* 1. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

* 1. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

Vulnerability scans are conducted every month using Tenable Nessus. Results are uploaded into Cyber Security Assessment and Management (CSAM)—the ED’s official repository of information systems, and provides the information assurance and program officials with a web-based secure network capability to assess, document, manage, and report on the status of IT for security authorization processes in the risk management framework in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). If any vulnerabilities are discovered, they are remediated within the specified time-frame based on severity. The system requires annual audits of security artifacts and controls to ensure proper National Institute of Standards and Technology (NIST) security controls are documented and in place.

# Auditing and Accountability

* 1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

Staff are provided security and privacy awareness and protecting information training as indicated in 7.4. Staff are made aware that the PII contained within NCRTM is for collection and maintenance and not to be distributed, exported, or printed. Staff sign rules of behavior regarding their use of the NCRTM and information contained within it. Monthly vulnerably scans and system audits are conducted to reduce the risk of outside threats obtaining the PII.

* 1. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

* 1. What are the privacy risks associated with this system and how are those risks mitigated?

According to the FIPS199 the security risk is low. RSA and contractor staff, systems and processes comply with National Institute of Standards and Technology (NIST) 800-53 controls for a Low Application which include administrative, technical and physical controls. These controls are in place to ensure integrity, availability, accuracy and relevancy of the data and to mitigate privacy risks. An unauthorized disclosure of the PII contained within NCRTM would cause a limited impact because it is not sensitive and is generally available publicly in other locations online. Grantee names, work email addresses, etc. are often available on their company/organization websites, in published works, in professional online directories, etc. Disclosure of the PII is not likely to cause identify theft and would likely, at most, have a limited, adverse effect on individuals. Additionally, an unauthorized modification of information in NCRTM would cause a limited impact. Information processed by the NCRTM contains no sensitive information or information that is not publicly available. The issuance of improper information could be detected elsewhere and would not damage public confidence to such a severe degree that the Department would not be trusted to complete this business function or result in a financial impact over $3 million over 3 years.

1. The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB Circular A-130, page 33](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf) [↑](#footnote-ref-1)
2. A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. <https://connected.ed.gov/om/Documents/SORN-Process.pdf> [↑](#footnote-ref-2)
3. Examples include restricted form filling, account verification, editing and validating information as it’s collected, and communication with the individual whose information it is. [↑](#footnote-ref-3)
4. If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section. [↑](#footnote-ref-4)