Privacy Impact Assessment (PIA)
for the

Rehabilitation Services Administration Management Information System (RSAMIS)
May 27, 2022

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Jack Johnson/IT Specialist
Contact Email: Jack.Johnson@ed.gov

System Owner

Name/Title: Jack Johnson/IT Specialist
Principal Office: Office of Special Education and Rehabilitative Services (OSERS)

Please submit completed Privacy Impact Assessments to the Privacy Office at 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.

1. Introduction

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

Rehabilitation Services Administration (RSA) grantees, including State vocational rehabilitation (VR) agencies, client assistance programs, and Protection and Advocacy of Individual Rights (PAIR) programs, use the RSA Management and Information System (RSAMIS) to report information regarding performance and expenditures under RSA formula and discretionary grants. RSA staff use the RSAMIS to analyze these data and administer the programs. The RSAMIS consists of three components:

1. A component which collects and disseminates performance and financial reports across RSA programs. Grantees submit reports through a form on a web portal; these reports are later reviewed within the portal by RSA staff. This component does not collect any PII other than the names of individuals submitting reports.

2. A component that allows State VR agencies to upload the Case Service Report. The Case Service Report is an information collection tool used to assist in administering the VR and supported employment (SE) programs. This component collects PII including name, Social Security number (SSN), date of birth (DOB), demographic information (e.g., sex, race, disability characteristics), services and training received, health insurance, disability information, benefits information, educational information, employment status, employment outcomes, earnings, ex-offender status, other barriers to employment.

3. A database server accessed by Department employees to process, query, aggregate, and store the information in RSAMIS, including the above-mentioned PII.

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

[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

RSAMIS maintains PII for program performance, accountability, research, monitoring, and evaluation purposes. RSA staff use the RSAMIS to analyze data received from grantees and administer programs in which grantees participate. The PII collected by RSA is required by the Rehabilitation Act of 1973, as amended by Titles I and IV of the Workforce Innovation and Opportunity Act (WIOA).

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

This PIA is being updated as part of a regular biennial review.

1.5. Is the system operated by the agency or by a contractor?

Agency

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

☑ N/A

Click here to select.

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific 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.

The RSA was established by Congress as the principal Federal agency authorized to carry out Titles I, III, VI, and VII, as well as specified portions of Title V of the Rehabilitation Act of 1973, as amended by Title IV of WIOA. RSA collects data in accordance with Sections 101(a)(10), 106, and 607 of the Rehabilitation Act (29 U.S.C. §§ 721(a)(10), 726, and 795l).

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

Case Service Report (RSA-911) SORN (18-16-02), published in the Federal Register on July 30, 2020.

2.2.2. 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.

☑ N/A

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. 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.

The Department shall submit a retention and disposition schedule to NARA for review that covers the records contained in this system. The records will not be destroyed until such time as NARA approves said schedule.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

[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

3. Characterization and Use of Information

Collection

3.1. 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.

Individuals with disabilities receiving VR and supported employment services from State VR agencies: name, SSN, DOB, demographic information (e.g., sex, race, disability characteristics), services and training received, health insurance, disability information, benefits information, educational information, employment status, employment outcomes, earnings, ex-offender status, other barriers to employment, username, and password.

RSA grantee representatives: name and organization.

Federal employees and contractors: username and password.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The PII collected and maintained is the minimum amount required by RSAMIS. RSAMIS maintains PII for program performance, accountability, research, monitoring, and evaluation purposes. RSA staff use the RSAMIS to analyze data received from grantees and administer programs in which grantees participate. The PII collected by RSA is required by the Rehabilitation Act of 1973, as amended by Titles I and IV of the WIOA.

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

PII is collected from State VR agencies and grantee representatives submitting reports. The agencies collect PII directly from individuals who are participating in or have exited the VR and SE programs.

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

The PII is submitted as part of quarterly reports which are securely uploaded to RSAMIS by the VR agencies.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

When the file is submitted to RSA, RSA runs the file through a series of logic-based edit checks. Any errors identified by these checks are then provided to the VR agency via email.

Use

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

RSA collects PII for performance accountability provisions in Title I of WIOA. WIOA requires that RSA reports on the primary indicators of performance, established in Section 116, based on characteristics of the VR program participants who are being served, including but not limited to sex, age, and race/ethnicity. The data elements collected by VR agencies and reported to RSA allow for this reporting. RSAMIS uses PII for program performance, accountability, research, monitoring, and evaluation purposes. RSA staff use the RSAMIS to analyze data received from grantees and administer programs in which grantees participate. The PII collected by RSA is required by the Rehabilitation Act of 1973, as amended by Titles I and IV of the Workforce Innovation and Opportunity Act (WIOA).

Once collected from VR agencies, the data is also shared with the U.S. Social Security Administration (SSA), pursuant to section 131 of the Rehabilitation Act, to monitor and evaluate programs serving individuals with disabilities. Under the established memorandum of understanding, SSA will match RSA's annual file of data to SSA program records to create a matched data set that will be used for authorized research projects.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

[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.

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

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.

3.8. 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.

Yes

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

□ N/A

The SSN is necessary for SSA to confirm the identity of the individual.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

□ N/A

While alternatives were considered, the collection of SSNs is required to satisfy statutory requirements related to data sharing with SSA.

4. Notice

4.1. 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, etc.)? If notice is not provided, explain why not.

Since the Department does not collect information directly from individuals, the Department does not provide direct notice to individuals regarding the collection of their information. State VR agencies are required to inform individuals being served by their programs that their information is being collected and provided to the Department.

Public notice is provided through the publication of this PIA and the SORN referenced in 2.2.1.

4.2. 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.

☑ N/A

4.3. 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 with disabilities who are receiving services from a State VR agency are required to provide PII (e.g., disability status information) to the State VR agency.

4.4. 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?

☑ N/A

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

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

☑ N/A

External

5.4. 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.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

□ N/A

RSA shares PII collected with SSA for data-matching purposes with SSA records. PII shared with SSA include: SSN, DOB, demographic information (e.g., sex, race, disability characteristics), services and training received, health insurance, disability information, benefits information, educational information, employment status, employment outcomes, earnings, ex-offender status, other barriers to employment.

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

□ N/A

Pursuant to section 131 of the Rehabilitation Act, PII is shared with SSA to monitor and evaluate programs serving individuals with disabilities. Under the established Memorandum of Understanding (MOU), SSA will match RSA's annual file of data to SSA program records to create a matched data set that will be used for authorized research projects.

5.7. Is the sharing with the external entities authorized?

□ N/A

Yes

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

□ N/A

Yes

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

□ N/A

[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.

An annual file is electronically transferred to SSA via secure file transfer.

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

□ N/A

Yes

5.11. Does the project place limitation on re-disclosure?

□ N/A

Yes

6. Redress

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

If an individual wishes to gain access to their record in the system of records, they can contact the system manager at the address listed in the SORN. The individual must provide necessary particulars such as name, DOB, SSN, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. Requests by an individual for access to a record must meet the requirements of the regulations in 34 CFR 5b.5, including proof of identity.

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

If an individual wishes to change the content of a record regarding their information in this system of records, they must contact the system manager at the address listed in the SORN and provide name, DOB, SSN and any other identifying information requested by the Department. The request must also reasonably identify the record and provide a written justification for the change. Requests to amend a record must meet the regulations in 34 CFR 5b.7.

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

Individuals are notified in the published SORN about the procedures for correcting their information.

7. Safeguards

If you unsure which safeguards will apply, please consult with your ISSO.

7.1. 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

7.2. Is an Authorization to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

□ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

RSA employees who can access the database have approved Privileged User Agreements (PUAs) in place and the necessary security clearance levels to do so. Access to this system will require a unique user identification as well as a password to access the system. Users will be required to change their passwords periodically, and they will not be allowed to repeat old passwords. Any individual attempting to log on who fails is locked out of the system after three attempts. Access after that time requires intervention by the system manager. The system limits data access to Department and contract staff on a “need to know” basis and controls individual users' ability to access and alter records within the system.

The server is located in a secure room, with limited access only by those who are authorized to access. Further, all physical access to the site where the server is maintained is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.

In addition, cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transmission.

7.5. 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

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

Yes

7.7. 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.

The RSAMIS database is scanned weekly, and the information is provided to various application owners. There is a patching process in place where patches are downloaded from vendor supported repositories and reviewed by administrators before a regularly-scheduled implementation. Patches are applied first in non-production environments and allowed to operate for a week as a test before application to production environments.

Additionally, RSAMIS is required to be granted an ATO on a tri-annual basis. This process includes a rigorous assessment of security controls, a plan of action and milestones to remediate any deficiencies, and a continuous monitoring program between the full scope assessments.

8. Auditing and Accountability

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

The system owner works with the Department's Privacy Program to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document.

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

Yes

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

Privacy risks associated with RSAMIS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, encrypting PII stored in the database, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate these risks, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating device operating software, amongst other software updates. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.