REHABILITATION SERVICES ADMINISTRATION (RSA)
PAYBACK INFORMATION MANAGEMENT SYSTEM (PIMS)

WHAT YOU NEED TO KNOW REGARDING SECURITY INCIDENTS

What is a security incident?

A security incident, or data breach, is a violation or an imminent threat of a violation of security policies, acceptable use policies, or standard security practices. Security incidents involve the disclosure or potential disclosure of Personally Identifiable Information (PII), which is information that can be used to distinguish or trace an individual's identity.

- Examples of PII include:
  - Social Security Number (SSN)
  - Driver's License Number or State ID Number
  - Passport Number

What are some examples of security incidents that have happened in the PIMS?

- A scholar or grantee sends the PIMS Help Desk an unencrypted email or file that contains PII, such as a photo of a Social Security card or driver's license.
  - **If this happens, the email or file with PII could be intercepted and potentially lead to identity theft.**
- A grantee uploads a Payback Agreement or Exit Certification form with the SSN visible to the wrong scholar record.
  - **If this happens, a scholar will be able to view the SSN and other identifying information of another scholar.**

What happens if a security incident occurs?

Every security incident that occurs requires significant resources from the U.S. Department of Education (Department) to mitigate the impact:

1. PIMS staff notify the Department's Education Security Operation Center (EDSOC), document the incident, and work to expunge the file or email from the PIMS or email servers.
2. Additional interviews, investigations, and mitigation strategies might be necessary if an unauthorized individual viewed the PII.
3. PIMS staff must review all other scholar records and documentation associated with the grantee to ensure other security incidents have not occurred.

Grantees are also impacted by security incidents. If multiple incidents occur, **the grant and university could be placed on high-risk status, affecting their ability to receive future federal funding**. Project directors and staff will also be required to participate in the following activities:

- Department investigation as needed, including the completion of the security incident report documentation and investigation interviews
- PIMS security training to understand the proper handling of scholar PII and the consequences of data breaches

How can I prevent security incidents from happening?

1. Minimize the use of PII in emails.
2. If PII must be sent via email, send the information in an encrypted (password-protected) file and then send the password in a **separate** email.
3. Implement a file naming convention to avoid uploading the wrong file to a scholar's record (e.g., Agreement_J_Doe.pdf).
4. Develop or use a file upload checklist to ensure that scholar agreements have:
   a. The correct scholar name,
   b. The SSN redacted, and
   c. An accurate file name.
5. Open the file after uploading to verify that the correct scholar record corresponds with the file.

What does the Help Desk do to prevent security incidents and data breaches?

- Help Desk staff verify they are communicating with the correct individuals via phone or email by confirming the user's identity using two pieces of information (e.g., email address and date of birth).
- Help Desk staff do not provide login instructions to any user without confirming the user's identity.

Where can I find more information?

- Additional resources regarding security incidents and other topics can be found on the PIMS Training and Resources Page located at **https://pdp.ed.gov/RSA/Home/Training** and the FAQs are available at **https://pdp.ed.gov/RSA/Home/faq/**.
- For general information on U.S. Department of Education cyber security guidance, please visit the **Handbook Chapter on Record Keeping, Privacy, and Electronic Processes**.
- For more information on U.S. Department of Education security incident protocol, please visit the **Privacy Technical Assistance Center's Data Breach Response Checklist**.
- If you have any other questions or need further assistance, please contact the Help Desk at **RLTTHelpDesk@ed.gov** or call 1-800-832-8142. The Help Desk is staffed Monday through Friday from 8 a.m. – 8 p.m. (Eastern).