



Considerations for the Secure and Responsible Management of RESEA Evaluation Data

Adam Travis and Correne Saunders, September 2023



When designing and implementing evaluations of the Reemployment Services and Eligibility Assessment (RESEA) program, state agencies are appropriately interested in strategies for sharing data that protect the privacy and rights of Unemployment Insurance (UI) claimants participating in the study. This tip sheet outlines four key considerations for ensuring data security, in accordance with best practice, and federal and state laws including the Federal Policy for the Protection of Human Subjects, often referred to as the “Common Rule.”¹

Tip #1: When conducting an evaluation, engage with an Institutional Review Board (IRB) or work with an evaluator who has access to and experience working with an IRB, to develop appropriate data security procedures.

IRBs serve as independent and objective ethics committees that oversee research involving human subjects. IRB review and monitoring will help ensure sound data security practices for your evaluation (see Box 1 for a summary of key concepts). To this end, it is important to engage with an IRB early in the study design process, or work with an evaluator that has experience submitting an IRB application and complying with data security protocols. If you are conducting your own evaluation, start by reaching out to your state’s health agency to ask for guidance on whether the agency’s IRB can review your study. If you are working with a state university, ask to be connected with the university’s IRB. If you are working with a third-party evaluator, ask which IRBs they have worked with in the past, or whether they have their own IRB.²

Box 1. Key Terms

- **Institutional Review Board (IRB):** IRBs serve as independent and objective ethics committees that oversee research involving human subjects. IRBs review and monitor research to ensure that researchers are taking necessary steps to protect study participants.
- **Personally Identifiable Information (PII):** PII refers to information that can be used to trace a person’s identity that is not publicly disclosed nor publicly associated with the service or intervention received in a program. Examples of PII include names, Social Security numbers, birthdates, addresses, and other forms of contact information.
- **Privacy:** Privacy relates to the collection and use of personal information from study participants during the course of an evaluation. Limiting the amount of information collected from study participants to that which is necessary for the evaluation is one way to protect the privacy of study participants.
- **Confidentiality:** Confidentiality includes the protection of personal and private information from disclosures, including the steps that researchers take to securely store and analyze study data, as well as practices for protecting private information when reporting data and disseminating study findings.
- **Informed Consent:** The process of providing a prospective study participant with sufficient information for making a voluntary and informed decision about whether or not to participate in a study.

¹ Federal Policy for the Protection of Human Subjects, 45 C.F.R. § 46.101, <https://www.ecfr.gov/on/2018-07-19/title-45/subtitle-A/subchapter-A/part-46>.

² In cases where both an agency and evaluator both operate in-house IRBs, it might be necessary to

Typically, the process of engaging an IRB begins with an application that includes basic information about the study design, research questions, data collection methods, and study population. The IRB will use this information to determine what safeguards the project requires for ethical research. The IRB may consider the study's procedures for informed consent (if relevant), specific steps the evaluation will take to protect participants' privacy and confidentiality, the evaluation's data security plan, and protocol for managing risk and disclosures.

In general, most evaluations engaging human subjects that use federal funds must work with an IRB for a review of the study design, including data security procedures. The time required for an IRB review can range from weeks to months depending on the complexity of the study design and level of risk to study participants. The need for continued IRB involvement over the course of the study can also vary.

Tip #2: Establish data sharing agreements.

In most cases, state agencies will need to enter into a **data sharing agreement** before sharing data with evaluation partners. If a third-party evaluator is conducting your evaluation, the evaluator will typically take the lead on drafting this agreement. A data sharing agreement outlines the *specific data elements* that will be shared for the purpose of the evaluation, protocols for *secure file sharing*, limitations for *data use and storage*, *contact information* for the staff responsible for handling the data, and *requirements for the destruction* of shared data upon completion of the evaluation:

- *Specific data elements*: A data sharing agreement should include a list of UI claimant characteristics and outcomes that the evaluation will require in order to answer the research questions. This includes a data dictionary (if available) to locate where information about those characteristics and outcomes is stored in the program's information systems. The agreement should identify specific database names, variable names, and parameters (e.g., dates and program codes that identify the specific study population). It is important to consider whether and how data files can be linked together using a common identifier across files.
- *Secure file sharing*: A data sharing agreement should specify a secure process for the transfer of data files, such as the use of an encrypted file transfer protocol. (Sending data files via email is not secure.) The agreement should also specify how often data will be updated and shared, and how notifications will be sent to ensure data is received and processed in a timely manner.
- *Data use and storage*: A data sharing agreement should provide details on where study data will be stored and how access to the data will be limited to authorized users only. The agreement should specify specific access controls, such as how permissions to the data are provided and managed over time, firewalls that are in place, and any additional protections such as anti-spam or anti-malware tools. If data will be accessed remotely, describe security measures such as using a VPN, a secure file transfer portal, encryption, two-factor authentication, or others.³ The

obtain approval from both IRBs. In cases where neither the evaluator nor the agency operates an in-house IRB, commercial IRBs are also available for a fee. The Office for Human Research Protections at the U.S. Department of Health and Human Services (HHS) maintains a database of registered IRBs that have conducted research supported by HHS: <https://ohrp.cit.nih.gov/search/search.aspx?styp=bsc>.

³ Many research organizations adhere to guidance from the National Institute of Standards and Technology (NIST) for minimum security controls, specifically Federal Information Processing Standard (FIPS) 200 (<https://csrc.nist.gov/pubs/fips/200/final>) and the Federal Risk and Authorization Management Program

agreement should also name a data custodian or primary point of contact for each party to the agreement and should identify the authorized users who will be able to access the data. The agreement should also include a clear protocol for how to handle unintentional disclosures or incidents.

- *Data destruction:* A data sharing agreement should clarify how to handle data files upon the conclusion of the evaluation. Typically, researchers delete data files containing personally identifiable information (PII) or other potentially sensitive information at the conclusion of the study or at some specified time-point thereafter. The agreement should include details on whether to keep a de-identified public-use data file for future use or dissemination (see Tip #4).

Tip #3: Omit PII or other potentially sensitive client information that is not needed for the evaluation from shared data file.

When creating or sharing data files for your RESEA Evaluation, only include information and data elements that are absolutely necessary for the evaluation. Some PII fields may be necessary for linking records across different administrative databases. Depending on a study's research questions and data needs, however, many forms of PII may be unnecessary. For example, an evaluator likely does not need study participants' street addresses or phone numbers in order to analyze program participation and reemployment outcomes unless participant contact is part of the evaluation. States should request a justification from research partners for specific data elements to ensure that they are not sharing more information than is necessary for the evaluation.

Whenever a third-party evaluator or other study partner requests data extracts that includes PII, they should specify why the PII fields they are requesting are necessary for the evaluation. In some cases, it might be possible to use non-PII data items to consistently identify or link to study participants' records. For example, each study participant might be assigned a unique identifier (e.g., Case ID, Individual Record Number) not tied to their Social Security number. Such non-PII identifiers could be used in many data extracts sent to an evaluator.

In general, requesting a justification for all requested data fields is also a good practice for non-PII data elements. In some cases, non-PII data fields can, in combination, be used to identify specific individuals. Asking for a justification for all requested data fields can help ensure that agencies are not sharing more information about study participants than is necessary for the purposes of the evaluation.

Tip #4: Plan to produce a public-use data file that can be safely shared with DOL, independent researchers, and members of the public after the evaluation has concluded.

Most data sharing agreements and data security plans will outline a process for destroying all sensitive evaluation data (especially data that contain PII) at the end of the study. If possible, include a requirement in your evaluator's scope of work that includes the creation of a **public use file**. A public use file is a fully de-identified data file. That is, it should not be possible to use the information contained in a public use file to identify specific individuals. Public use files are maintained for archival purposes, or for subsequent analyses by state or program staff, other researchers, or members of the public.

(<https://www.fedramp.gov>). NIST also provides many good resources on implementing controls to protect sensitive data, including a list of trustworthy platforms and networks (<https://www.nist.gov/cybersecurity>).

The public use file should not contain any data elements that could be used to identify individual study participants. This includes PII fields such as name, Social Security number, date of birth, address, or contact information. In some cases, it might also include **indirect identifiers** that, in combination, could be used to identify specific individuals. Indirect identifiers might include geographic identifiers (such as Census tract) as well as information about participant race, ethnicity, or gender. For example, if a RESEA program only served a very small number of UI claimants who identified as Black or African American, providing information about participant race alongside other characteristics such as age and gender might make it possible to identify individuals in a dataset, even where PII such as name, Social Security number, and date of birth have been removed.

The level of disclosure risk posed by indirect identifiers will depend on the combination of data elements included in the data file as well as the level of detail provided by each data element. In some cases, categorizing variables such as age or income can lower disclosure risk by reducing the level of detailed information available about study participants.

ABOUT THIS SERIES

State agencies' evaluations of their RESEA interventions (i.e., the whole program or aspects of it) are integral to expanding the evidence base of effective service delivery strategies. This tip sheet is part of a series developed to serve as a quick-reference tool for states planning, launching, and carrying out evaluations of their RESEA programs.

Suggested citation: Travis, A. & Saunders, C. (2023). *Considerations for the Secure and Responsible Management of RESEA Evaluation Data*. RESEA Evaluation Technical Assistance Tip Sheet. Prepared for the U.S. Department of Labor, Chief Evaluation Office. Rockville, MD: Abt Associates.

Additional Resources and Information

DOL's RESEA Helpline: RESEA@abtassoc.com

Additional RESEA evaluation technical assistance resources are available here:

https://rc.workforcegps.org/resources/2019/07/30/17/32/RESEA_Evaluation_Evidence_Resources

Study reports, publications, and other materials are available here:

<https://www.dol.gov/agencies/oasp/evaluation/completedstudies/RESEA-Evidence-Building-Implementation-Study>

Chief Evaluation Office
U.S. DEPARTMENT OF LABOR



This document was prepared for the U.S. Department of Labor (DOL), Chief Evaluation Office by Abt Associates under Contract # 1605DC-18-A-0037. The views expressed are those of the authors and should not be attributed to DOL, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.