SRAENE

Sexual Risk Avoidance Education
National Evaluation

BEST PRACTICES FOR MANAGING AND STORING DATA – FREQUENTLY ASKED QUESTIONS

This document contains frequently asked questions that Sexual Risk Avoidance Education (SRAE) project teams might have as they plan and implement systems for managing and storing data. It is important to plan for data management and storage before collecting data so that evaluation teams know the procedures to keep and use data securely and safely. Collecting data from youth younger than 18 can be particularly sensitive. The type or source of data collected is the key driver in identifying and applying relevant safeguards related to security and confidentiality. This document answers questions that program leaders and evaluators might have related to collecting, transferring, storing, cleaning, and using data, and addresses the systems needed to securely manage and then properly destroy data.

What is personally identifiable information (PII)?

PII is any piece of information that directly or indirectly identifies an individual. PII includes:

- Name
- Social Security numbers
- Address
- Date of birth
- Personal email addresses
- Phone numbers

As part of your evaluation, you might collect PII on parent consent forms, youth assent or consent forms, surveys of youth or staff, or other data collection efforts.

Why is securely managing and storing data important?

Your partners and the youth you serve are trusting you to safeguard their information. If data are not securely managed and stored, someone's personal information or responses in surveys, focus groups, interviews, or other data sources might be revealed to others. This violates participants' confidentiality and threatens the integrity and ethics of your evaluation activities.

What is a data management plan?

A data management plan is a document that describes the procedures your team will use to ensure that data are managed and stored securely. The plan will help ensure consistency across your team, and you can use it during staff training as a resource. The plan doesn't need to be lengthy or complicated. In fact, it might be useful to create a plan that provides information through graphics or bulleted lists, so it is easy for staff to use.

What are some considerations when developing a plan for managing and storing data?

When developing a data management plan, keep in mind the particular details of your data collection methods, the structure or format of the data, and your planned analysis. Consider the following questions when developing a plan for managing and storing data:

- **How are we collecting the data?** The plans for managing and storing data will vary based on mode of data collection. For example, if you are collecting staff surveys via paper-and-pencil methods, your plans will need to address how you will securely manage the hard copies of the surveys, securely enter those data into an electronic format, and securely store the electronic data. Remember to consider qualitative data when developing your plan for managing and storing data; information collected from interviews or focus groups is also data and can include sensitive details.

- **What are some considerations for data that include PII?** If you are collecting PII, you will need to think carefully about storing the information in a protected and restricted location. Store paper copies that include PII in a locked cabinet or drawer. For example, do not leave documents like consent forms sitting on your desk or in a car. For electronic data, ensure that the information is stored in a protected and restricted folder on a secured drive. To keep PII secure, you will need to de-identify the data. This means creating a system to link a respondent's name with an ID number. The ID system is then stored in a secure location so that the project team never has data directly associated with an individual's name. The process of de-identifying data should occur shortly after collecting the data.

- **How do we get the collected data back to the evaluation team?** In some cases, staff and partners who collect the data need to transmit information back to the evaluation team. For example, if you are collecting student surveys on paper, you will need to develop a secure process to transfer information to your evaluator or evaluation team. You might transfer data securely through encrypted email or file transfer sites like Box. When transferring data, remove respondents' names and instead use ID numbers for individuals. Remember that emailing staff or youth's names without encryption is not secure, and teams should avoid transferring data via email without encryption.

- **What do we plan to do with the data after we collect them?** Teams usually need to clean or reorganize data before analysis begins. For the data management plan, consider the steps needed to get the data in a form that the evaluation team can analyze. For instance, if you are collecting data via online surveys or forms, look at a sample of the output and map out how the team will securely clean or reorganize the raw data to get the information you need to answer your research questions.

- **What clearances or other requirements do we need to consider when collecting data?** Each project will have varying clearances or requirements. In addition to local requirements, check with your federal project officer if you are unsure about the federal guidelines and regulations you must follow. The bullets below list different data security documentation, clearance, and training requirements.

  - **Data use agreement or memorandum of understanding.** When two partners enter a business relationship, they usually establish an agreement laying out the terms of that partnership. You might establish such an agreement with partners to collect data for your implementation evaluation—for example, forming an agreement with a school partner to share student attendance data with you. Several terms describe these types of agreements. Terms such as data use agreement (DUA), memorandum of understanding (MOU), memorandum of agreement (MOA), or data sharing agreement (DSA) all refer to an agreement put in place between your organization and an entity from which you are obtaining data, where there might be certain restrictions on using the data. These agreements often outline the terms of the agreement with respect to practices for managing and storing data.
  - **Background investigation or personnel security clearance as a prerequisite to working on the project or accessing data or systems.** Sometimes school districts require background checks for all staff who interact with minors. As such, you will want to ensure that all staff who will be working with youth have obtained the necessary security clearances. Check with the school and district in which you are offering programming to learn about their specific requirements before beginning data collection.
  - **Institutional Review Board (IRB) clearance or exemption.** IRBs review and approve research studies to confirm that study plans comply or are exempt from the Federal Policy for the Protection of Human Subjects. IRBs exist to ensure that research participants are protected. IRBs also ensure that the data collected from research participants are secure. For more information on IRBs, see this SRAENE resource or the resources on the performance measure portal's T&TA resources page.

- **How do we store data securely?** It is essential to protect and save data securely. You will need to develop a process to ensure the data are secure, and the processes will likely vary if the data are electronic or hard copy on paper. For example, for electronic data, consider who has access to your network folders and storage. For these types of data, avoid only storing them on a laptop or USB key that can be lost or stolen. For physical data, such as printed survey or fidelity logs, lock them in a storage cabinet or other secure location. Never store data in open areas.
- **How do we securely destroy data after we are done with them?** As part of your plan, consider what to do with the data after you have used them for their intended purposes. You might need to retain some records for a set amount of time. In other cases, you might need to destroy or dispose of data immediately in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying or disposing of paper records, especially those that include PII, are shredding or burning them. Your IRB often will provide guidelines about what to do with your data at the end of the study.