SRAENE
Sexual Risk Avoidance Education
National Evaluation

June 2023

Tip Sheet

OPRE Report No. #2023-158

Best Practices to Safely Store and Share Data

When collecting data, organizations need to plan how to store and share data safely and securely. Organizations offering SRAE programs might collect data about sensitive topics, such as sexual activity. Telling youth the information they share will be kept safe and secure can help youth feel they can answer questions honestly and improve the accuracy of the data collected. Organizations can set up clear protocols and procedures to maintain confidentiality and comply with standards for ethical data collection, such as those required by an institutional review board. The accompanying video introduced strategies that organizations can implement to safely store and transfer data. Read more about these strategies below and see Table 1 for definitions of key terms.

Maintain confidential and secure storage of electronic and paper data and information. You can maintain data confidentiality by securely storing all collected data in a manner that can only be accessed by staff with appropriate permissions to access the data. This can include paper or electronic survey data, notes from interviews or focus groups, and personally identifiable information (PII).

Safely transfer paper and electronic data. If you need to share data with evaluation partners or other entities, consider how you will transfer data securely. When transferring data to partner organizations, hard-copy and electronic data require different considerations for keeping them safe and maintaining confidentiality. Be sure to encrypt electronic data to ensure it remains secure.

Effectively destroy data when no longer needed. After analyzing the data or after a set time following program participation, your organization will no longer need to keep the data you have collected. At this point, you should dispose of data effectively and completely.

Address mishandled data or information leaks. Sometimes data are accessed or shared inappropriately. If an actual or suspected breach happens, make sure you notify your institutional review board right away. Check with your institutional review board on its timelines and requirements for notifications following breaches. Evaluate how the data were accessed or shared, so you can identify steps to resecure the data and put protections in place to prevent it from happening again.

Table 1. Key terms

Term	Description
Data destruction software	Resource used to completely erase data from a hard drive. When you delete files on a computer, it is not the information but the reference that is deleted. Data destruction software removes the data completely, ensuring it cannot be recovered.
Personally identifiable information (PII)	Information that could identify a specific individual, such as name, school, address, or phone number. For example, someone might be able to identify youth who completed a survey if they see their school and address information. Collecting data anonymously (e.g., without PII) can lower the risk of disclosure of personal information, though it may reduce the ability to track completed surveys or analyze data based on respondent characteristics.
Encryption	Form of securing confidential or proprietary information as it is transmitted or while it is stored digitally.
Institutional review board (IRB)	A group that oversees research on human subjects and ensures the research follows ethical procedures. All IRBs must be registered with the Office of Human Research Protection in the U.S. Department of Health and Human Services.
Secure data	Safeguarding information collected from respondents through security practices, procedures, and infrastructure. For example, safe data practices include never leaving completed surveys out where they could be viewed, storing electronic data in password protected files, and minimizing the number of staff with access to sensitive data.

For more on PII:

This video provides an overview of PII: https://www.dhs.gov/privacy-training/what-personally-identifiable-information

This webpage provides an overview of PII: https://www.dol.gov/general/ppii

For more on safe storage of data:

This web page provides an overview of best practices for data storage: https://ria.princeton.edu/human-research-protection/data/best-practices-for-data-a

For more on encrypting data:

This web page provides an overview of how to encrypt through Microsoft: https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7#

These web pages provide an overview on best practices for data destruction: https://studentprivacy.ed.gov/resources/best-practices-data-destruction, https://research.viu.ca/research-ethics-board/data-retention-and-destruction

About this series

This video series, and the accompanying tip sheets on understanding and collecting high-quality survey data, were created as part of the Sexual Risk Avoidance Education National Evaluation (SRAENE). The series covers a range of data-related topics to help grantees understand the importance of high-quality data and provide guidance on how they can collect them in their program. Although some of the resources are drawn from topic areas that are not related to SRAE, the content on data is still relevant.

FYSB does not recommend any particular survey platform or data system that may be referenced in tip sheets.

For more information or questions, contact the SRAENE team at SRAETA@mathematica-mpr.com.

Suggested citation: Tabackman, W., White, S., Eddins, K. (2023). *SRAENE – Best Practices to Safely Store and Share Data Tip Sheet* (OPRE Report No. #2023-158). Washington, DC: Office of Planning, Research, and Evaluation, Administration for Children and Families, U.S. Department of Health and Human Services.