SRAE Performance Measures Data Privacy and Security Requirements

Updated 05-28-2020

This document provides information on the required data privacy and security protocols for Sexual Risk Avoidance Education (SRAE) performance measures. Entry and exit performance measures surveys have been revised with some questions removed and changes to responses. Overall, the performance measures surveys address some of the following subjects:

- living situation (e.g., living with family [parent(s), guardian, grandparents, or other relatives]);
- use of alcohol, tobacco, or other drugs (e.g., cigarettes, alcohol);
- goal setting (e.g., doing well in school, graduating);
- healthy relationships (e.g., talking to a trusted adult when in an uncomfortable situation); and
- perceptions on the experience of the program (e.g., materials clearly presented, feeling respected).

In addition, collection of personally identifiable information (PII)—which includes any data that could potentially be used to identify a particular person, such as full name, date of birth, etc.—requires protection against unauthorized access.

Consequently, it is important to keep such data secure. The following sections describe required procedures for ensuring the protection of private information, including granting access to data, secure storage of identifying information, data transmission, submission of de-identified data to the SRAE Performance Measures Portal, reporting, and destruction of identifying information.

Access to Data

Access to SRAE performance measures data should only be granted to project staff who need access and who sign a confidentiality agreement. Staff responsible for data collection, data entry or scanning, and submission to the SRAE Performance Measures Portal need to sign confidentiality agreements because these activities involve access to the data. Other staff may not need access or may only need limited access. For example, facilitators may collect attendance data but may not need access to completed entry and exit surveys.

Secure Storage

Documents that contain PII (e.g., completed parent consent forms, youth assent forms, and rosters of youth with parent consent and who assented) must be stored in a separate, locked file cabinet and/or on a separate secure computer server from survey data.

Hard copies of completed surveys should be stored in a locked file cabinet. Survey responses should be separated from any PII. This can be done by:

- Not collecting PII on surveys;
- Collecting and recording PII separately (e.g., a roster) and using identification numbers on surveys; and
- Keeping completed surveys in a separate filing cabinet from rosters, consent/assent forms, and attendance sheets.

Electronic data files must be stored on a secure computer server or hard drive, and all computers and other devices must be password-protected with access to data granted only to project staff who need access to the data and who have signed a confidentiality agreement. Electronic data may also be stored on a secure CD or flash drive that is password protected and accessible only to staff who have signed a confidentiality agreement. Secure CDs and flash drives should be stored in a locked file cabinet. PII should be stored separately from survey data. This can be done by:

- Storing PII in a separate dataset from survey responses, in a different file and/or folder, or on a different CD or flash drive that can be accessed only by staff who need to know PII; or
- Locking hard-copy, consent/assent forms, rosters, and attendance sheets in a filing cabinet and using identification numbers in the electronic survey dataset.

Electronic data may be stored in the cloud as long as they are encrypted, password-protected, and accessed only on authorized computers that require password protection.

Local Data Transmission

When data collectors send hard copy, completed surveys to the grantee organization and/or local evaluators, these documents should be sent in a package marked confidential via U.S. Postal Service or Federal Express. An authorized signature and show of picture identification should be required before receipt. The sender must obtain a tracking number and follow up if data are not received. Documents including PII should be shipped separately using these same protocols.

When data collectors send electronic files to the grantee organization and/or local evaluators, these files will be transmitted via encrypted email, CDs, or flash drives. The secure shipping protocols above should be used when shipping CDs or flash drives. Passwords should be transmitted separately from secure files (e.g., in a separate email message, in a voicemail message).

Data submission to the Family and Youth Services Bureau will be through the SRAE Performance Measures Portal.

Submission of De-Identified Data to the SRAE Performance Measures Portal

Data submitted to the SRAE Performance Measures Portal biannually should not include PII about youth participants. Detailed guidance for submitting data to the portal will be provided in June 2020.

Reporting

Reports about performance measures data should not include any information about individual youth respondents. To minimize the risk of identifying individual youth by their responses, cell sizes smaller than 10 respondents should use data suppression techniques or not be reported.

Destruction of Performance Measures Data

Documents that include PII or survey data should be destroyed in a secure manner (e.g., shredding hard copies, deleting electronic files) after three years.