SRAEPAS
Sexual Risk Avoidance Education
Performance Analysis Study

Required Data Privacy and Security Protocols

SRAEPAS
Sexual Risk Avoidance Education
Performance Analysis Study

GOAL

Secure all data

- Personally identifiable information
- Participant data
- Sensitive organizational performance measures data

PERSONALLY IDENTIFIABLE INFORMATION (PII)

- Any data that could potentially be used to identify a particular person, such as
  - Full name
  - Date of birth
  - E-mail address
  - Driver's license number
- Any unauthorized access or release of such information could result in severe consequences for the individuals whose data have been compromised.

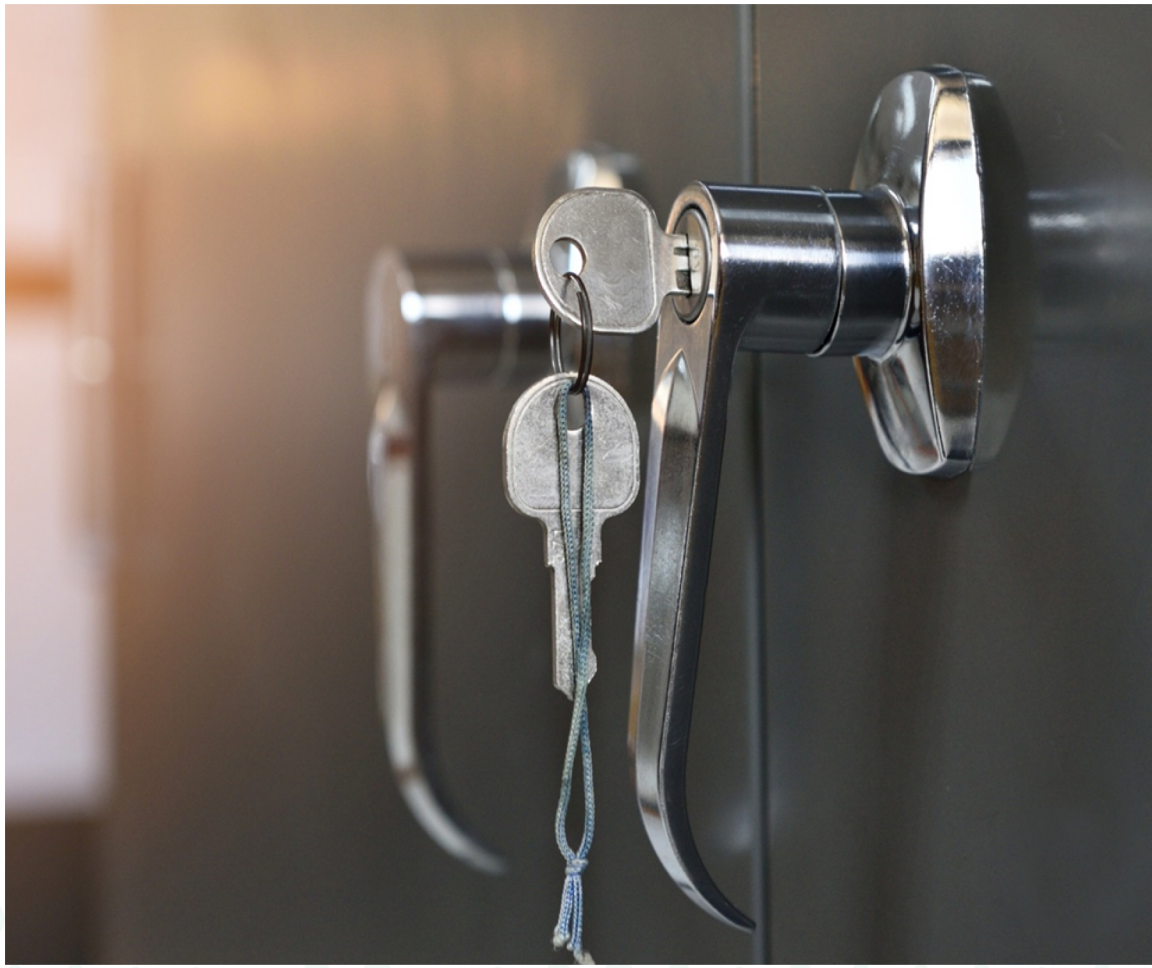
ACCESS TO DATA

- Identify who will have access to the data, based on their need to know
  - For example, facilitators may collect attendance data but may not need access to entry and exit survey response data
  - Staff responsible for data collection, data entry or scanning, and submission through the portal will need access to the data
  - Evaluators who are helping with program evaluation
- Require signed staff confidentiality agreements

SRAEPAS
Sexual Risk Avoidance Education
Performance Analysis Study

HARD COPY DATA STORAGE

- Use a locked filing cabinet
- Separate survey responses from any PII. This can be done by:
  - Not collecting PII on surveys
  - Collecting and recording PII separately (e.g., a roster) and use identification numbers on surveys
  - Keeping completed surveys in a separate filing cabinet from rosters, consent/assent forms, and attendance sheets



ELECTRONIC DATA STORAGE

SRAEPAS
Sexual Risk Avoidance Education
Performance Analysis Study

- Use password-protected shared drives
- Grant access only to authorized staff with signed confidentiality agreements
- Store in the cloud as long as data are encrypted, password-protected, and accessed only on authorized computers with password protection
- Keep survey response data separate from any PII. For example, this can be done by
  - Storing PII in a separate dataset from survey responses, in a different folder that can be accessed only by staff who need access to the PII
  - Locking hard copy consent/assent forms, rosters, and attendance sheets in a filing cabinet and using identification numbers in the electronic survey dataset

LOCAL DATA TRANSMISSION

HARD COPY DATA

- When data collectors send completed surveys to the grantee organization and/or local evaluator:
  - Ship PII separately from survey responses
  - Send in packages marked confidential via U.S. Postal Service or Federal Express
  - Require an authorized signature and show of picture identification before receipt
  - Obtain tracking number to follow up if data are not received
- Data submission to FYSB will not involve hard copies

ELECTRONIC DATA

- When data collectors send completed surveys to the grantee organization and/or local evaluator:
  - Use encrypted e-mail, CDs, or flash drives
  - Follow same protocols for shipping hard copy data when shipping CDs or flash drives
  - Transmit passwords separately from data
- Data submission to FYSB will be through the SRAE Performance Measures Portal