PMAPS
PREP Studies of Performance Measures and Adulthood Preparation Subjects

PREP
Performance Measures

Data Privacy and Security Guidelines

This document provides guidelines for data privacy and security protocols for Personal Responsibility Education Program (PREP) performance measures. The performance measures participant entry and exit surveys address some potentially sensitive subjects, including sexual activity, contraceptive use, incidence of pregnancy and sexually transmitted infections, and whether youth are in foster care, experiencing homelessness, or in adjudication systems. In addition, although the performance measures do not include participants' names or other personally identifiable information (PII), grantees and partners involved in collecting the data might have access to this information.

It is important to keep such data secure, and PREP grantees and subrecipient providers are responsible for ensuring the privacy of participants' data. The following sections provide guidance for protecting private information, including guidance on restricting access to data, secure storage, local data transmission, submitting data to the PREP Performance Measures Management System (PMMS), reporting, and destroying data.

Access to data

Access to PREP participant performance measures data should be granted only to project staff who need access and who sign a confidentiality agreement. Staff responsible for collecting, entering, scanning, or submitting data to PMMS should sign confidentiality agreements because these activities involve access to the data. Other staff might not need access or might need only limited access. For example, facilitators could collect attendance data but might not need access to completed entry and exit surveys.

Secure storage

Staff should securely store documents that contain PII (such as completed parent consent forms, youth assent forms, and rosters of youth) separately from survey data.

Staff should store hard copies of completed surveys in a locked file cabinet. Survey responses should be separated from any PII. This can be done in several ways:

- Not including PII on surveys
- Recording PII separately (for example, a roster) and using identification numbers on surveys
- Keeping completed surveys in a separate locked file cabinet from rosters, consent or assent forms, and attendance sheets

Staff should store electronic survey data files on secure computer servers, hard drives, compact discs (CDs), or flash drives. Electronic storage should be password-protected and accessible only to project staff who (1) need access to the data and (2) have signed a confidentiality agreement. Staff should secure CDs and flash drives in a locked file cabinet. PII should be stored separately from survey data. This can be done in two ways:

- Storing PII in a separate data set from survey responses, in a different file and/or folder, or on a different CD or flash drive that only staff who need to know PII can access
- Keeping hard-copy rosters, consent or assent forms, and attendance sheets in a locked file cabinet and using identification numbers in the electronic survey data set

Staff can store electronic data in the cloud as long as the data are encrypted, password-protected, and accessed only on authorized computers that require password protection.

Local data transmission

When data collectors send completed hard-copy surveys to the grantee organization or local evaluators, they should send documents in a package marked confidential and require an authorized signature and picture identification before receipt. The sender should obtain a tracking number and follow up if the data are not received. Staff should ship documents including PII separately from surveys, using these same protocols.

When data collectors send electronic files to the grantee organization or local evaluators, they should transmit these files via encrypted email or password-protected CDs or flash drives. Staff should use the secure shipping protocols described in the previous paragraph when shipping CDs or flash drives. They should transmit passwords separately from secure files (for example, in a separate email or voicemail message). Data submission to the Family and Youth Services Bureau will be through PMMS.

Submitting aggregate data to PMMS

Data submitted to PMMS biannually will not include PII. Webinars conducted shortly before each data submission window begins will provide detailed guidance for submitting data to PMMS.

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.

Destroying performance measures data

Staff should destroy documents that include PII or individual-level participant survey data in a secure manner (such as shredding hard copies and deleting electronic files) after five years.

Additional information about the Personal Responsibility Education Program (PREP) performance measures is available at www.prepeval.com. For further support, contact the Mathematica PREP Performance Measures technical assistance team at PREPPerformanceMeasures@mathematica-mpr.com or call toll-free 1-855-267-6270.