Appendix Q2. Data Security Plan

This page has been left blank for double-sided copying.

Data security plan

To be responsive to FNS requirements regarding respondent protections, research staff will sign the Confidentiality Pledge (Appendix Q1) and participate in annual security awareness training. The confidentiality pledge stipulates sanctions for noncompliance and complete online security awareness training shortly after their start date. The contractor's Human Resources group monitors training completion and compliance through an online training portal, which generates a certificate of completion and records the user's completion score.

Access to the data will be limited to members of the study team working directly on the study or with oversight responsibilities, except as otherwise required by law.

The study team will ensure that data are secure by providing a secure transfer site for administrative data from States and local agencies and storing all study data in a restricted access project directory on a password-protected local area network. Participants will be assured that the information they provide will not be released in a way that compromises privacy or data security. The contractor's servers are located behind their firewall and housed in a locked data center located in the contractor's locked, access-controlled office suite. Sensitive data resides on a project-specific folder accessible only to research staff with a business need-to-know, as restricted by identity-based policies and access control lists. The data is encrypted as it is stored on the server with an AES 256-bit key, which is Federal Information Processing Standards (FIPS) 140-2 compliant. The data is mirrored in a secure, fault-tolerant data center; only authorized Mathematica Information Technology Services staff have physical or logical access to the data mirror. Snapshot backups of the data are taken periodically throughout the day and stored on the data mirror. Sixty days after data is securely deleted from the primary server, the

backup data mirror is automatically and securely deleted, a process that enables compliance with secure data destruction requirements.

Any portable media containing sensitive data are secured with Advanced Encryption Standard (AES) 256-bit encryption. Project staff are instructed to remove sensitive data from their desks when not in use or when unauthorized staff or visitors are present. Research staff will employ the server's secure delete features to permanently purge electronic data as required. Any backups will also be securely deleted 60 days after primary files are purged. De-identified data may be archived for later use.

The web surveys will be developed in Confirmit, a computer-assisted survey software package developed by the company of the same name, and all data will be stored securely within this system. Through Confirmit, unique user credentials (ID and Password) are created for each survey participant. Each participant will be assigned to a copy of the instrument. Access to the instrument is provided via a URL sent to the participant's email account. The URL will contain an embedded hashed ID and Password for the participant. When the participant clicks on the URL, they will be automatically directed to the website and authenticated into the instrument. All data captured through Confirmit, will be stored in a study-specific folder that is encrypted with AES 256-bit encryption on the Confirmit server. All access to this data is controlled by Active Directory groups on Mathematica's Domain Network. Each study team member must have valid credentials to access the Confirmit data stored in restricted access folders. While none are expected, any hard-copy documents submitted will be physically secured in locked storage cabinets and shredded at the close of the study.

While the survey requests contact information to allow the study team to follow up with respondents to clarify responses, personally identifiable information (PII) will not be used to retrieve survey records or data. Neither the survey nor the other data collection materials in this collection require a Privacy Act Statement. Contact information will be stored with the other study data in a restricted access project directory on a password-protected local area network and will not be shared outside the study team.