

Appendix G-1 Data Management Security Protocols

Data management security protocols ensure restricted access to data and confidentiality of data maintained on the system and in reports. For example, Optimal Solutions Group, LLC (Optimal) uses secure intranets to maintain project-related files, and its secure servers use industry-standard methods, such as firewalls, monitored access logs, virus protection, encrypted connections, password-protected accounts, and user authentication mechanisms, to ensure the confidentiality of the survey design, test data, and subsequent analyses. Optimal maintains a biometrically secure environment and employs a data security officer who oversees Optimal's data. All Optimal staff members are trained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance, with re-certification completed every 2 years. To support the development and delivery of services, Optimal has made significant investments in a flexible and effective technology infrastructure to ensure the communication, accessibility, and security of information and the ability to submit deliverables in a timely and effective manner.

System Environment

The security approach used to protect the restricted-use data (RUD) is based upon Defense in Depth principles. Security protections have been designed to address controls relative to people, technologies, and operations with technologies focused on defending the network or perimeter, the enclave, the computing environment, and the supporting structures. In general, the RUD enclave consists of a single web portal accessible only via a virtual private network (VPN) and remote desktop software. The server does not have access to the World Wide Web, nor does it have public IP addresses open. Access is only granted via the secure VPN connection. Power continuity is provided by a state-of-the-art 8-hour uninterruptable power supply that will ensure that back-up power systems will provide ample capacity to keep servers running during any generator failure. Upon contract award, Optimal drafts a data security plan with input from SBA.

FTPS

Optimal uses a secure file transfer protocol server (FTPS) to transfer data between an end-point, such as a user's workstation, and Optimal's data server. FTPS utilizes a cryptographic protocol called Secure Socket Layer (SSL), which provides secure transmission of data over a file transfer protocol (FTP). Optimal's FTPS meets standards set forth by Federal Information Processing Standard (FIPS) publication 140-2. The cryptographic module used by Optimal's FTPS server is a FIPS 140-2 validated cryptographic module that meets the highest possible security standards. End users can connect to Optimal's FTPS using a variety of secure FTP clients. Each user that connects to Optimal's FTPS will have a unique username and password, and will only have access to their own data. Access logs are kept for security review purposes. The server that runs FTPS is protected by a firewall, anti-virus protection, and protocols designed to restrict access to the server in order to maintain security.

In order to securely transfer data to Optimal, an FTP client that supports FTPS (FTP over SSL) is needed. Many commercial FTP programs support FTPS. If someone does not have any FTP software on their computer, Optimal can provide information on downloading and using an FTP client. In the event of uncertainty of whether someone's software is capable of FTPS, Optimal's technical assistance team should be contacted for assistance. Optimal's technical assistance team will also ensure that the FTP client is set up properly and is operating in a secure, HIPAA-

compliant mode. All file transfers between sponsors, and Optimal's data server meets Centers for Medicare & Medicaid Services and Department of Health and Human Services requirements by complying with HIPAA requirement 164.312(e)(1) Transmission Security, and by using a validated FIPS 140-2 cryptographic module.

Secure Servers

Optimal operates several secure servers to meet the data security needs of various projects. These servers are protected using industry standard methods, such as firewalls, monitored access logs, virus protection, and encrypted connections to each server. Data can be analyzed using statistical packages and other applications located on each server, eliminating the need to move the data to an unsecure location. The STATA and SPSS software, for example, are running in a secure, virtual environment. These software programs can be used to analyze and report on a wide variety of datasets. Running on remote servers allows the data to be analyzed from a single location by authorized Optimal employees from a variety of locations.

Furthermore, Optimal's servers used to access, transmit, receive, or store electronic protected health information (ePHI) are located in a physically secure environment with 24/7 surveillance and monitoring. All system accounts are password-protected and user authentication mechanisms are implemented to control user access to the system. Optimal employs a security patch and update procedure that ensures that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected. Optimal's servers are located on a secure network with firewall protection. The only network access to the servers allowed is through a secure VPN connection. All unused and unnecessary services are disabled on the servers.

Optimal will conduct analyses on the electronic data in several ways. All analyses will be conducted on Optimal's secure data server, which meets HIPAA's administrative, physical, and technical guidelines for storing, transmitting, and accessing ePHI and other sensitive information. Optimal employees will connect to Optimal's data server using a secure VPN. Data analyzed for the project will stay on Optimal's secure data server and will not be downloaded to any workstations. Optimal will use server-based STATA and SPSS to analyze the data. Analyses generated will be exported to a database, also hosted on Optimal's data server, for reporting purposes. Optimal will perform qualitative analyses on raw and analyzed data. Results of these analyses will be entered into Optimal's database and will be used for reporting purposes.

HIPAA

Optimal ensures data security and integrity by strictly adhering to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security guidelines. Optimal's employees are trained in HIPAA security and HIPAA awareness. Server and workstation security requirements ensure that PHI and other sensitive information are handled properly at all times. Sensitive data are encrypted during transmission and storage. Physical and virtual access to secure data is monitored, controlled, and only granted on an as-needed basis.

Optimal performs a rigorous, ongoing HIPAA risk-assessment process. Optimal's risk assessment committee identifies security and HIPAA risks throughout the organization. From there, the committee works to mitigate any risk to an acceptable level. Results of the risk assessment process are stored for reporting purposes.