AppendixA-2. Optimal Solutions Group, LLC Data Security Protocols

Data management security protocols ensure restricted access to data and confidentiality of data maintained in information systems and in reports. 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 data collection, test data, and subsequent analyses. Its security protocols were designed to fulfill obligations of the Privacy Act and Office of Management and Budget circulars and memorandum. 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 Sensitive But Unclassified (SBU) or proprietary business data 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. Optimal’s systems are tailored to the security level of the data being housed or transferred. Whether through a vendor or locally hosted, the system environments meet best practices for physical and environmental controls as outlined by the National Institute of Standards and Technology. For example, power continuity is provided through redundancies to ensure that back-up power systems will provide ample capacity to keep servers running during any generator failure; signed access rights forms are required for changes to the limited staff assigned to each project and system; and Optimal maintains a biometrically secure environment and employs a data security officer who oversees Optimal’s data and security policies.

File Transfer

Optimal uses a range of proven file transfer methods depending on the requirements of the project. Cryptographic protocols such as Secure Socket Layer (SSL) or Transport Layer Security (TLS) are in place and a minimum of AES 256 encryption is used. Optimal's protocols meet standards set forth by Federal Information Processing Standard (FIPS) publication 140-2. End users can connect to Optimal's servers using a variety of secure FTP clients or other interfaces. Each user that connects to Optimal's systems has a unique username and password, and only has access to his or her project data. Access logs are kept for security review purposes.

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, encrypted connections to each server, and passwords that require changing every 90 days. 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 R software, for example, are running in a remote, 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. All unused and unnecessary services are disabled on the servers.

In cases where data cannot be maintained on a network, the necessary software is installed for use on a standalone PC without a connection to the Internet. It may allow access to a local server and/or allow physical access to the room, depending on the requirements of the project. Furthermore, Optimal's locally hosted servers used to access, transmit, receive, or store highly sensitive information such as 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.

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.