DATA SECURITY PLAN

The NHCS Data Security Plan (DSP) describes the survey procedures and data handling protocols that are implemented to secure study data and protect confidentiality. The plan follows the structure and guidelines established by the National Institute of Standards and Technology (NIST; 800-series)[1] for meeting the requirements of the Federal Information Security Management Act (FISMA).[2] The DSP complies with all relevant laws, regulations, and policies governing the security of data and the protection of confidentiality, including the Privacy Act of 1974 (5 USC 552a), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) (44 USC 101), and Section 308(d) of the Public Health Service Act (42 USC 242m).

The overall objective of the security policies and practices summarized in this document is to protect the NHCS systems and data from a wide variety of threats that could compromise the confidentiality, integrity, or availability of the data. This is accomplished by implementing and monitoring a wide variety of security controls, as specified in NIST SP 800-53, Revision 3. These standards and guidelines specify over 150 data security controls in 17 different data security topic “families.” These topic areas address a broad range of risks, including employee screening and training, building or plant security, information system access, and software vulnerabilities, among others. This Data Security Plan summarizes our policies and practices for a subset of the most relevant controls.

The NHCS DSP considers all known data security and confidentiality protection risks. However, our approaches and specific procedures will evolve as we identify new data security threats and implement improved practices. A record of updates to the DSP is given at the end of this document. The updated plan is reviewed and approved annually.

Subcontracting staff who work on NHCS are required to comply with the same security standards as Westat staff, an agent of NCHS.

Personnel Security

Each Westat employee and contractor is instructed in and required to comply with Westat’s data security policies, standards, and procedures through staff orientation programs and by the employee/contractor’s manager/supervisor. In addition, all staff must complete Westat’s Information Security Awareness Training annually. Items covered include password administration, transmission or delivery of data files, and printing and handling of materials containing confidential data, such as field materials, reports, or frequencies. All Westat employees and contractors are required to read and pledge compliance with Westat’s "Employee or Contractor’s Assurance of Confidentiality of Survey Data." In addition, all staff working on

[1] See http://csrc.nist.gov/sec-cert/ca-compliance.html.
[2] See http://csrc.nist.gov/policies/FISMA-final.pdf.

NHCS must have completed the NCHS Confidentiality Training and signed the NCHS Nondisclosure Affidavit.

All Westat staff members undergo, at a minimum, a Federal or state government and/or Westat-procured background screening check at least once every 3 years (or every year for more sensitive Westat positions). When a staff member leaves the company, appropriate steps are taken to transfer responsibility and preserve any data to which the user may have access. Terminating employees with certain access privileges may be given alternative assignments and their access privileges suspended upon notice of eventual termination. The day a staff member departs, his/her building access card is deactivated. Any computer accounts assigned to the user are deactivated to ensure that the departing employee no longer has access to project directories or network resources. If the staff member has a key to a secure room or a PC containing sensitive data, the locks are changed.

Media Protection and Data Transfer Control

Data files transmitted from participating NCHS hospitals to Westat will occur through Westat's secure data network (SDN). FIPS 140-2 validated Advanced Encryption Standard (AES) encryption is used both for file transfer and for protecting files while they are temporarily stored on the data transport server. Access to the system is controlled through the issuance of individual usernames and complex passwords. All file transfer and administrative actions are logged into an audit trail, and data files are overwritten with random bytes once they have been deleted. Once files have been received by the Westat secure data network, they are downloaded into a secure, limited-access network directory for verification and editing. This directory is located in a separate internal network security zone that is isolated by firewall settings from incoming connections from the Internet.

Appropriate administrative and technical safeguards are also employed to protect the security of all sensitive and confidential NHCS information on digital (laptops) and non-digital (paper) physical media, including the following:

- All data stored on laptops are encrypted using FIPS 140-2 compliant encryption (PGP).
- NHCS data being transmitted between field laptops and Westat office servers are protected both by FIPS 140-2 compliant file encryption and by the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS).
- Protected Health Information (PHI) is included in files and on paper survey materials only when necessary to complete a particular task.
- Access to computer files containing PHI is limited to those staff with a specific need for the information.

- System-generated output containing confidential data is stored in locked areas until no longer needed and is disposed of in accordance with NHCS requirements.
- Electronic media such as CDs that contain data which is no longer needed are destroyed by degaussing, low-level formatting, shredding, or other industry-approved destructive methods.
- For paper records that need to be destroyed, Westat provides both stand-alone paper shredders and designated secure paper recycling containers at various locations throughout the campus.

System/Data Access Controls

All NHCS project data are stored on network file stores or on database servers. Access to these secure computer systems is password protected. All server and network data storage areas are protected by access privileges, which are assigned by the appropriate system administrator. Login passwords are encrypted and stored only in their encrypted form in protected files on each system. A non-displaying or non-printing feature prevents the password from appearing on the computer screen during the login process. The system automatically limits the number of unsuccessful attempts to log in, after which the account is disabled and must be reset by the system administrator. Passwords must be of a minimum length, must meet certain character and numeric usage rules, must be changed periodically, and cannot be reused. Accounts that have not been used for 90 days are automatically disabled and deleted within 1 week upon notifying relevant managers.

Building/Physical/Environmental Protection

Access to Westat facilities is controlled at all times through the use of magnetic key cards assigned to individual staff, certain contracted consultants, and, in a few approved cases, selected vendor staff with established long-term business relationships. In addition, all staff are issued photo identification cards which must be visibly displayed at all times. Every use of the magnetic key card to enter a particular building or area is recorded in an electronic log for security and tracking purposes. Visitors are required to sign in with a receptionist and receive a day pass.

Access to the computer centers is also controlled by the key card entry system, with limited access privileges for designated operations and project support staff only. These specially designed centers house the computer systems, equipment for data communications, network services and operations, and high-speed printers. Special secured areas are established for sensitive data processing functions such as storing and printing of confidential data based on project requirements.

Westat buildings are protected against fires by automatic smoke detection and overhead sprinkler systems, in accordance with local building and fire codes. These systems are centrally monitored by a fire panel that automatically dispatches the local fire department to arrive within minutes at our location in the event of an alarm condition. Computer facilities are equipped with redundant air conditioning systems to control temperature and humidity and are monitored 24 hours a day, with alarms providing notification of any abnormal conditions. Computer facilities are also protected against electrical power surges and short-term outages by battery-based uninterruptible power systems (UPS) and against fire by a chemical fire suppression system specifically designed to reduce the risk of damage to computer equipment and storage media that would result from a water-based system. Diesel-powered backup generators support the continuous operation of the data centers in case of long-term utility power failures.

Audit and Accountability

All information systems at Westat capture sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. Audit records are periodically reviewed for indications of inappropriate or unusual activity, and findings are reported to appropriate officials who take any necessary corrective actions.

Data Backup and Storage

Westat's Computer Operations staff backup all server-based storage to tape on a daily basis. All backup tapes are removed daily from Westat's premises and transported in secure containers to an off-site storage facility that specializes in transporting and storing electronic media. Tape identifiers for all backup tapes are maintained in a central tape management system for easy reference and retrieval.

Data File Preparation and Delivery

NHCS deliverables containing identifying or other sensitive information will be delivered to NCHS using CDC’s Secure Data Network (SDN). If delivery over the SDN is not possible due to file size or some other reason, data files will be encrypted and written to CDs or DVDs. The media containing the encrypted files will either be hand-delivered or sent by registered, tracked delivery service (such as FedEx) to the NHCS Project Officer or designated representative.

Data Archiving and Disposal

All NHCS data files will be returned to NCHS or destroyed at the conclusion of the project. While the project is underway, Westat’s Archive Tracking System (WATS) is used to manage the archival, retention, and retrieval of both electronic data and hardcopy materials. The WATS system includes a manager notification and corporate archivist review procedure for all archive and retrieval requests. In addition, WATS maintains a historical log of all project archive activities for future reference if necessary. Archive materials are sent off site to a reputable and bonded external secure data storage firm for safekeeping. Project materials are kept for the duration of the retention period specified at the time of archiving. When the retention period has expired, the owner of the materials is contacted to confirm that they are no longer needed.

Following this confirmation, the materials are securely destroyed (shredded or burned or magnetically erased).

Data Security Incident Reporting

All staff working on NHCS are required to report security incidents in which they believe systems security has been, or may be, breached, such as by the unauthorized or suspicious presence of unidentified individuals on Westat premises; the unauthorized use of passwords; unauthorized access to a server area or otherwise secure systems area; the demonstrated or likely existence of a virus on a computer; and possible unauthorized transmission of confidential data without encryption or security. Any actual or suspected breach, theft, loss, or potential loss of confidential information will be reported to the NCHS Chief Information Security Officer and the NCHS Confidentiality Officer within one hour of discovery.

Software System Development/Acquisition

NHCS follows a defined life cycle methodology that includes information system security, defining information security roles and responsibilities, and assigning individuals to those roles. Security is considered in all phases of the system development life cycle and treated as an integral part of the system development and implementation process, including system modifications. The system manager and development team leader ensure that adequate and effective management, operational and technical control mechanisms are integrated into the system development lifecycle.

Westat acquires systems and services in the performance of its contracts for the federal government under the terms specified in those contracts and with Contracting Officer Authorizations (COAs). Security expenditures are incorporated into the capital budget planning process and includes investments in network security, expenditures in upgrades and enhancements in system security technologies, investments in security trainings for staff, investments in allocating staff resources for security responsibilities, and expenditures for testing corporate and project level business continuity/disaster recovery procedures. Westat’s Software Policy describes the rules governing software usage restriction and user installed/special use software. Westat also employs policies and procedures to ensure that adequate security protections are provided, enabled and tested for applications purchased from third-party vendors.

Software System and Information Integrity

Westat performs vulnerability scans weekly on servers to identify possible vulnerabilities. Results are made available to the appropriate systems technical administrators and managers who are required to respond with information on any corrective actions taken.

As a further measure, Westat periodically monitors traffic between each internally defined network security zone (i.e., internal sub-networks whose traffic is mediated by the firewall). This activity recognizes the pattern of common types of suspicious traffic that may indicate attempts by an internal or external user to access a specific computer for which the user is not authorized.

Server and workstation operating systems are updated with applicable security patches as they are made available by the vendors. Systems support staff subscribe to several nationally recognized security alert services to keep informed about current and emerging security issues or product vulnerabilities as they are made known. Procedures are in place for staff to respond to early warnings about security threats whether during or outside regular business hours. Westat’s response protocol includes immediate action to gather information, protect systems, inform users, and take any new protective measures, such as applying newly released security software updates.

To protect PCs, email services, and network data storage facilities from damage caused by viruses and worms, Westat scans local PCs, network servers, and all email messages for possible viruses and worms. All networked PCs are required to use Westat-installed anti-virus software, which scans files for viruses before saving them to the network. All incoming and outgoing email is scanned, and any suspicious messages are quarantined for possible follow-up investigation. In addition, network disk storage areas are scanned in real-time mode and again once each night. The anti-virus scanning software is updated and distributed to network servers, email servers, and PCs automatically on a scheduled basis to ensure that currently reported viruses will be detected. Urgent updates can also be "pushed" to all servers and PCs between the scheduled times, when necessary to prevent the spread of a recently discovered virus.

Plan Implementation and Enhancement

Westat is committed to observing high standards of information technology (IT) and systems security in order to protect systems and data from a wide range of threats that could affect the confidentiality, integrity or availability of data, to comply with the various legislative and contractual requirements of our clients, and to educate our staff regarding their responsibilities to comply with these policies. Security for NHCS is a joint effort involving project management, project IT staff, and corporate support units and staff. Security policies, procedures, and documents are reviewed at least annually by the System Manager and other senior project management, and are amended or supplemented in response to new industry developments in IT security and relevant security risks or events that may arise from time to time.

Westat's Corporate Officer for Systems Security (COSS), reporting to the President, oversees the development and application of company information technology and systems security policies and best practices, and monitors conformance to these policies and best practices throughout the organization. The COSS also maintains an online archive of systems security information, including relevant detailed memoranda, instructions, and external reference documents, to guide and assist staff in planning and implementing systems security.

Updates to the NHCS DSP

Date	Version	Updated By	Description
11/2/2011	1	Mike Rhoads	Initial version