DATA SECURITY PLAN

The NHDS Data Security Plan (DSP) describes the survey procedures and data handling protocols that will be 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), Section 308(d) of the Public Health Service Act (42 USC 242m) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, PL 107-347) of 2002.

The NHDS 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. The DSP will be updated before each subsequent phase of the project with more detailed, process-oriented data security protocols. The updated plans will be developed, reviewed, and approved before the Pretest and two main survey phases.

Pretest and National Survey Phase Data Security Plan

The overarching strategy for securing NHDS project data is to reduce our vulnerability for data loss and to protect the sensitive data that we do collect with rigorous data protection procedures. Vulnerability is reduced by limiting the collection and use of sensitive, or personally identifying, data to the essential survey data requirements or management tasks and eliminating their use for all other activities. We implement rigorous data protection procedures by following the NIST data security standards and guidelines.

The NIST standards and guidelines require the implementation and monitoring of hundreds of 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. In this Pretest and national survey DSP we provide a summary of the NHDS specific data security controls that will be implemented. These controls are a subset of the full set of controls that are required in the NIST standard and that will be implemented for the project. These data security controls will be updated, and more specific protocol-level details will be provided in subsequent Data Security Plan updates. The set of NHDS data security controls cover the areas discussed below.

---

1 See http://csrc.nist.gov/sec-cert/ca-compliance.html.

2 See http://csrc.nist.gov/policies/FISMA-final.pdf.

Project Staff

NHDS project staff including contractors and consultants and any new hires will be required to sign the NCHS Nondisclosure Affidavit and view the NCHS DVD "*Confidentiality Practices for Federal Employees and Contractors*" annually. The signed affidavits and a record of compliance will be sent to NCHS and stored in the project management system. NCHS will be notified immediately of any new hires during the period of performance.

RTI also requires confidentiality protection affidavits and annual security awareness training for all staff. RTI operates in a NIST-directed data security standard environment which requires data security awareness training for all staff that is similar to the NCHS DVD mentioned above. This is an E-training video that RTI staff are required to view each year. In addition to the security awareness trainings, RTI project staff will receive survey activity specific data security training tailored to their responsibilities. Patient data abstractors, for example, will receive extensive training on the data security protocols for, among other activities, handling case folders, entering and transmitting data, and managing their laptops.

Media Protections

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

- Data stored on digital media are encrypted at a level to satisfy FIPS: 46-2 data encryption standard (RTI uses Pointsec to encrypt all laptop hard drives).
- Use of PHI on hard-copy survey materials will be limited to that which is absolutely required to complete the task.
- Respondent identifying information will be stored separately from research data and never used as an identifying field for a data record.
- Access to physical media storage areas is controlled and the media are secured when not in use.
- Physical media are sanitized (digital erase, or shredded) prior to disposal.

System/Data Access Controls

Only authorized staff will have access to the NHDS systems or data. System and data access security controls include: user identification and authentication rules, strong password requirements, system messages that explain authorization limitations and the ramifications of misusing project data, and active monitoring of system/data use and access.

Data Transfer Controls

Abstracted data will be transferred to the RTI secure network and deleted from the laptop as quickly as possible, and no more than 48 hours from the time the data were entered. Electronic data transfer will be protected with 128-bit SSL encryption. Guidelines will be enforced for transferring physical media that include the necessary package receipt checks and other security protections.

Building/Physical/Environmental Protection

RTI security staff limits physical access to systems and to equipment to authorized individuals, protect the physical plant against environmental hazards, and provide environmental controls in facilities. NHDS project staff will prepare guidelines for providing a secure workspace to abstract medical records and require that all fieldwork be accomplished in this secure environment.

Audit and Accountability

RTI information system personnel create, protect, and retain information system audit records for the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

Data Backup and Storage

NHDS project data will be backed up and written to tape each evening. The backup tapes will be stored offsite in a secure concrete and steel reinforced media vault. The storage facility will be monitored 24 hours a day by an independent security firm.

Data File Preparation and Delivery

NHDS project staff will separate and store separately all personally identifying information collected for a patient. These data will be linked to other abstracted data via a random link identifier. Final data files will be written to encrypted stand-alone data storage devices that will be hand-delivered to the NHDS Project Officer.

Data Archiving and Disposal

Data archive contracts will be established that ensure the safe transport and storage of archived materials. RTI will also implement standard data disposal procedures for secure disposal of survey materials.

Data Security Incident Reporting

An effective incidence response protocol will be developed that emphasizes the importance of reporting potential problems immediately and provides a streamlined communication and response plan. These plans will be developed for the Pretest phase of data collection.

Personnel Security

RTI ensures that individuals in positions of authority are trustworthy and meet security criteria, that information and information systems are protected during personnel actions, and that formal sanctions for personnel failing to comply with security policies and procedures are enforced.

Software System Development/Acquisition

RTI employs system development life cycle processes and software usage and installation restrictions to protect information applications and services.

Software System and Information Integrity

RTI identifies, reports, and corrects information and system flaws in a timely manner, providing protection from malicious code, and monitoring system security alerts and advisories.

Plan Implementation and Enhancement

The data security protocols and procedures implemented for NHDS are developed, implemented, and maintained by the survey task managers in consultation with data security experts and the Project Director. Engaging project staff and relevant data security experts in the process of developing and maintaining the plan helps ensure that the survey protocols and task implementation plans are dynamic, continually improve in response to new threats, and always comply with relevant laws, regulations, and policies governing the security of data and protection of confidentiality.

The implementation strategy for the DSP recognizes that project staff members collecting or managing sensitive data are both the most vulnerable for losing or misplacing these data and the most able to identify potential problems and effective solutions. The NHDS DSP emphasizes training for project staff so that they are aware of the data security risks and can follow best-practice survey protocols for combating them. We also purposely empower project staff to identify new and improved methods for securing data and to communicate their ideas and suggestions directly to their Task Leader and/or the Project Director.

Data security experts will continually help shape and improve the Data Security Plan. The following corporate resources will assist in the implementation and enhancement of the DSP:

- **Protection of Human Subjects Committee**—RTI’s Institutional Review Board (IRB) will review all survey protocols to ensure that adequate protections are provided.
- **The Industrial Security Office** will implement the employee screening process for NHDS project staff.
- **The Corporate Security Office** will provide physical security including programs for protection of personnel, prevention of property loss, and protection of intellectual property and confidential information.

- **The Information Security Office** will review electronic security processes and provide technologies and services to protect the confidentiality, integrity, and availability of information technology resources.