Appendix D

1. DATA SECURITY PLAN

1.1 Overview

This document outlines RTI's plans for protecting the security and privacy of data collected as part of the Health Center Patient Survey (HCPS). All of the information collected will be private; some of the information is or may be considered sensitive. The sensitive information will include:

- household income and receipt of benefits;
- dates of birth;
- substance use, mental health status, and perceived need for services and utilization of services; and
- HIV/AIDS infection status and testing status.

This information will be collected as part of a field survey using laptops that are password-protected. In addition, the laptop's hard drive is also encrypted with Check Point Endpoint. Endpoint is a hardware encryption application required on all RTI corporate laptops to protect proprietary and confidential information from loss or theft. Endpoint uses mathematical functions to encrypt hard-drive information such as the operating system, resident data, temporary files, deleted files, and any unused space. Endpoint encryption is Federal Information Processing Standard (FIPS) 140-2 compliant. If a laptop is lost or stolen, the risk of data exposure is very small.

In addition, as part of routine survey administration, interviewers will carry paper forms for recording respondent consent and receipt of incentives. The use and handling of paper signed consent forms will be among the issues discussed with the Internal Review Board prior to data collection. Paper documents other than the consent form and the contact summary report form will not identify the study name nor content so that a respondent's personal information cannot be linked to study participation. The consent form will have the study name and the respondent's signature. The contact summary report form will contain case specific information along with

- date and time of contact attempt;
- outcome code (e.g., refusal, language barrier); and
- notes (e.g., respondent reluctant).

The use of paper forms carries a greater risk of data loss because the forms are more easily lost and publicly accessible than laptops. For this reason, we have limited the information collected on paper forms to the information that is absolutely necessary. Recording the results of contact attempts on paper forms facilitates its accuracy and accessibility.

We have designed the data collection protocol to minimize the amount of sensitive and identifying information that is stored on paper forms. Moreover, we have specified physical safeguarding and shipping procedures, as well as protocols for training interviewers in the use of these procedures. Completed paper forms are stored in project-provided laptop bags secured with a combination lock. These procedures are described in the remainder of this document, along with our procedures for network security, data processing and management systems, electronic data storage, and data transfer.

1.2 Network Security

RTI has implemented an Information Security program based on the Defense in Depth concept. This strategy combines the capabilities of people, operations, and technology. The first layer of protection is RTI's Internet firewall, which connects RTI to the Internet. All traffic between the RTI network and the Internet passes through this single connection point, providing a high level of protection to and monitoring of all systems within the RTI network.

The firewall is programmed with a set of rules to determine if network access is in compliance with RTI's network security policy and then allows or prevents access to the RTI network. The firewall logs all incoming traffic from the Internet to the RTI network. This information is essential in detecting and analyzing any problems.

The firewall allows interviewers to connect from outside RTI to use e-mail and exchange data through Web services, while databases and other servers remain at a higher level of protection. Access to the network from the Internet is very restricted, using a limited set of protocols into specific systems. The network is configured to provide services that require access from the Internet such as Web servers. Servers must be registered with RTI's Information Technology Services (ITS) department and must specify which services they run. This enables the firewall rules to allow only those requests for a particular service to pass through the firewall. All PII data will reside in the RTI's Enhanced Secure Network (ESN). Access to resources in the ESN requires two-factor authentication using an RSA token. E-mail and Web service access do not require two-factor authentication; however, no PII data will be sent via e-mail and all data sent to or received from the Web services are encrypted with FIPS 140-2 compliant encryption.

Web servers are placed behind load-balancing devices, which are configured to deny all traffic not specifically allowed according to their configuration. This serves as a layer of protection between the network connecting the Web servers and the rest of the network. Only approved file types are allowed on the Web servers. For example, CGI scripts are not permitted on Web servers. The load-balancing devices also perform Network Address Translation (NAT), providing another layer of protection to the Web server.

Computer-based tools are used to detect and identify vulnerabilities on RTI systems. This ensures that vulnerabilities, if detected, can be corrected before unauthorized persons exploit them. Multiple layers of automated network and server monitoring quickly identify failures or unusual activity levels, which may be an indication of an attempted security breach. Alerts may be sent 24 hours a day, 7 days a week via e-mail and pager to on-call staff for evaluation and resolution.

System and network administrators are automatically subscribed to multiple mailing lists to ensure they are quickly informed of security advisories. These include CERT, Microsoft, Network Associates, Trend Micro, Red Hat, and SANS. RTI is an active member in InfraGard, a cooperative security program between the Federal Bureau of Investigation (FBI) and commercial enterprises.

A multilayered antivirus program is in place. All e-mail is scanned entering and leaving RTI’s network. Antispam filters are in place. An additional layer of protection takes place at individual workstations, each of which runs antivirus software with automatic updates.

Security awareness articles are posted on the internal RTI Web site several times a year to ensure that staff remain aware of and vigilant about following appropriate security precautions, and specific alerts are issued when imminent threats are anticipated.

A standard IT security awareness training course is provided to RTI staff and contractors with an RTI Private Network user account. Employees complete this training within 30 days of hire and once annually thereafter.

ITS security staff maintain certifications including:

- Certified Information Systems Security Professional (CISSP) and
- firewall vendor certifications for administrators and engineers.

1.3 Data Processing and Management Systems

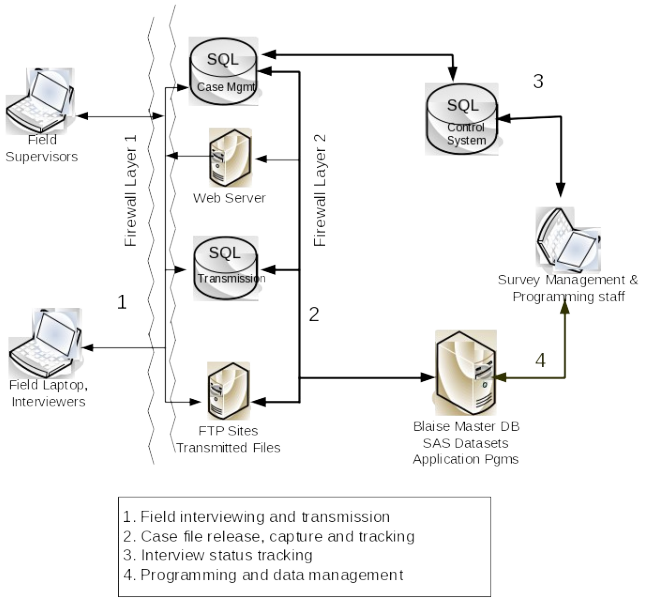
RTI will take appropriate precautions at all stages of data storage and handling to prevent disclosure, damage, or loss of study data. The major components of the data processing and management systems are:

- Control system—interface and database for use by RTI staff on the internal intranet to manage documents, case status, and contact information.
- IFMS—Web site and databases for use by field supervisors and RTI survey managers to assign and track cases in the field. Includes processes to receive incoming data and move it to the internal network.
- Blaise instrument—developed on the internal network and executed on field laptops to collect survey response data.
- Master response database—located on the internal network accessible only by RTI project staff, storing the collected response data from all completed interviews.

Utilities, reports, and data analysis applications—run nightly or on demand to produce reports for the Field Supervisors (FSs) and RTI survey managers.

Figure 2-1 presents an overview of how all of these systems tie together to produce an integrated and comprehensive data management system for the project.

Figure 2-1. BPHC Patient Surveys Data Management System



In general, data will be maintained on internal network shares or databases as needed until the close of the contract. Access to the internal network is only available to RTI employees, and access to project-specific shares is limited to team members for this project. The ability to update, delete, or change the data file storage area will be restricted to network domain managers and to staff approved by the project director. As a result, direct access to data is very limited. Most users can only access data through the secure data processing and management systems.

For privacy and security, RTI data processing and management systems use:

- unique identification numbers for cases, which are used in reports instead of recognizable personal information;
- data storage on RTI's internal, firewall-protected network;
- restricted access to network data through Windows authentication and share access lists;
- interviewer authentication in data collection systems and encrypted hard drives on laptops;
- encrypted file transmission through secure File Transfer Protocol (FTP) and Secure Socket Layer (SSL) encryption for the field management Web site. Specifically, before transmitting back to RTI's ESN via secure FTP, data are encrypted using a FIPS 140-2 module (cert #1330). Once received and validated, all data will be moved to project shares with strict access-control or stored in SQL Server databases. Data in the ESN, stored in the databases or project shares are not encrypted;
- nightly data backup with offsite storage for 3 months;
- up-to-date virus protection on all internal and external servers, workstations, and laptops; and
- password protection and role-based authorization on Web sites, case management systems, and control systems.

Authorized project staff can only access stored data from workstations that meet RTI's security standard. Each is protected from virus attack by regularly updated antivirus software. Data files are stored on workstation hard drives only while being worked on. They are deleted as soon as the activity is completed. Workstations are locked and password-protected when unattended and are located within keycard access buildings. Remote access is allowed through use of RTI-approved virtual private networking software for approved staff only.

1.4 Data Storage

All electronic data are securely stored on either file servers or SQL Server databases within RTI's secure intranet, as ***Figure 2-1*** shows and as described in the section on network security. Access to these servers will require login authentication and be

limited to staff on the project with a need to know. The project maintains two categories of data:

- response data from interviewing and
- tracking and control data for managing systems and schedules.

Of these, the response data require the highest level of security. Tracking and control data typically do not contain sensitive information, being linked to respondents only through internally assigned identification numbers.

Response data, once received from the field, are maintained in a Blaise master database residing on a secure file server. Access to this data is limited to in-house project staff and is controlled by Windows authentication and security group. The process of transferring response data from field laptops to RTI is described in the next section, Data Transfer. Tracking and control data are maintained in a SQL Server database. Again, this information is only available to in-house project staff with access to the control system.

The data stored in the IFMS system are primarily for field management operations and data transmission between field laptops and the data processing and management systems.

Examples of field management–related data are case assignment, production monitoring, and expense reports. Transmission data may include assigned cases, complete cases, case status, and transmission status. The IFMS data will be stored in a SQL Server database protected by SQL Server security and the more general network security enforced by access permissions and firewall protection.

The IFMS database will be used by the field supervisors, the project survey specialist, and the data collection task leader. Access to this database is via a secure Web site. The Web site has a current SSL certificate and requires a user- and project-specific username and password that filter the display of information on screen according to the role assigned to each user. For example, survey staff accessing the IFMS will see more information and options than the FSs. Very limited information is available to the FSs—mostly tracking information and summary reports.

SQL Server databases and file servers that are involved in transmissions to and from the field are programmatically accessible to field staff but not to the general public. The SQL databases contain tracking information identified by internally assigned case IDs, and they do not contain respondent contact or response data. Access to the databases is limited to authorized project staff and system

administrators. Other transient data, including case data for field interviewers or response data files sent back to RTI, pass through the secure FTP server temporarily via a SSL connection. Only project-authorized system administrators and programmers have direct access to the FTP file storage site.

Laptops used by FSs and Interviewers receive contact data and return response data, and thus the highest level of security must be applied to the hardware and processes. All field laptops run Windows 7 or XP with login/password protection. In addition, the hard drives of all laptops are fully encrypted and cannot be accessed by anyone who should happen to steal or otherwise obtain access to a project laptop. On startup, only the correct login will allow decryption of the laptop contents.

Data files and information stored on servers will be protected and maintained as long as the project needs access. Following the termination of the project, or following the end of the useful life of the information, files will be compressed, encrypted and archived to permanent media such as compact disk (CD) or digital video disk (DVD) for storage. CD and DVD archives will be maintained and stored in locked filing cabinets in the offices of project staff as long as needed, with destruction at the end of the study at the request of HRSA. Archived data is encrypted with FIPS 140-2 compliant encryption.

1.5 Data Transfer

There are several processes that will move study data within and outside RTI. These processes are shown with numbered arrows in ***Figure 2-1*** and include

- creation and transmission of preload data files for interviewing (processes 1 and 2);
- transmission of response data files from the field to RTI (processes 1 and 2); and
- sample loading, data management processes, reporting, and other internal operations (processes 3 and 4).

At each stage of information transfer, precautions are taken to ensure data safety and privacy. Only approved survey staff can access the file servers and databases, through login/password-controlled applications and Windows authentication.

Data transfer within RTI's secure intranet takes place under Windows authentication and access control lists, providing access only to staff specifically authorized for this project and to network administrators. Please see ***Section 2.2*** for details of internal network security.

In these ways, RTI will ensure the safety and privacy of data while it is stored and while it is in transit between the project team and members of the field staff.

1.6 Security of Electronic Data in the Field

Interviewer laptops will contain case IDs that link to other case management information such as the respondent's name, address, future contact information, and interview data. In addition to the protocols described previously, security measures are in place for protecting electronic data in the field:

- Laptops are strongly encrypted and password protected.
- Interviewers must transmit data to RTI every day that they work and at least three times a week. Interview data must be sent to RTI on the day they are collected. Field data are encrypted using a FIPS 140-2 module (cert #1330) before being sent to RTI's ESN via secure FTP. Once received at RTI and backed up, interview data will be deleted from the laptop. Supervisors will monitor interviewer adherence to the protocol using daily transmission reports.
- In the event a laptop is lost or stolen, only active cases and those awaiting deletion are on the laptop. With the laptop security procedures including encryption, as described in previous sections, the risk of these cases being exposed is very small.
- Passwords must not be written down or shared with anyone.
- When with a respondent, interviewers take care that the respondent cannot see the case management display on the computer, which may list other cases.
- All e-mail communication by field staff must take place using computer accounts established for the PHCPS (i.e., no use of personal e-mail accounts is allowed).

1.7 Safeguarding Physical Materials in the Field

Field staff will be trained on the importance of maintaining privacy of all study materials containing case-specific information, including the laptop computers themselves. Specific procedures designed to ensure that physical security of these items is not compromised include the following:

- When in the field, case materials must be kept with the interviewer or kept out of sight in a locked vehicle. However, materials may not be left in a vehicle overnight. No materials may be left visible in an unoccupied vehicle.
- When traveling, confidential materials must be carried on board the aircraft, not checked through baggage. In hotel rooms, materials must be kept locked and out of sight when not in use.

1.8 Shipping Materials

To prevent opportunities for data loss after an interview is completed, field staff will be held accountable for adhering to the specified procedures for shipping materials to RTI:

- Completed consent forms, incentive receipts, and contact summary report forms are shipped to FSs weekly. The FSs perform a quality-control check of all materials, and then ship the materials to RTI. After a period of observation confirming adherence to procedures, Interviewers may ship completed materials directly to RTI per their FS's direction.

- Field staff prepare a transmittal sheet and place it in the Federal Express package. The transmittal sheet contains the air bill number, name of the person who will receive the package, date the package is sent, and the case identification numbers of the case folders. Interviewers keep a copy of the transmittal sheet. If a package is lost, an inventory of missing items is readily available.

- Traveling field staff are not allowed to FedEx case materials from or to hotel addresses. Instead, they are expected to carry all case materials with them in their carry-on luggage or drop materials off at a manned FedEx station before traveling home.

- Field staff are instructed to send Federal Express tracking information via e-mail to their FSs each time they ship study materials to RTI. This e-mail must include a list of the items in the Federal Express package, the shipment date, the expected delivery date, the delivery address, and the tracking number. No respondent personally identifying information is included in these e-mails.

- Shipments among staff (e.g., materials associated with a transferred case) must be documented in e-mail between the two Interviewers involved and their FS(s). If the package does not arrive on the date expected, it will be tracked immediately. Packages cannot include the name or acronym of the study anywhere on the package or on the shipping bill.

1.9 Storage of Documents

Paper forms will be received, logged, and stored at RTI's Fulfillment Department. This controlled-access department resides inside a secured facility located a short distance from RTI's main campus.

- A small team will be assigned to the project and trained on procedures for receipt and storage of materials. These staff (along with all project staff) will sign the project's Data Privacy Agreement.

- All paper forms will be logged into the project's control system. This system will contain the case identification number and the status code of each case as well as contact information.

- Documents will be stored in locked filing cabinets.

1.10 Field Staff Training

Comprehensive training on all data privacy and security protocols will be provided to interviewing staff, as follows:

- The Field Interviewer (FI) manual will contain detailed information on all data privacy and security protocols, including requirements for safeguarding information, data transmissions, and shipment of materials. The FI manual also includes a description of disciplinary procedures for failure to follow project protocols, including those related to data privacy and security.

- The FI home study will include multiple items related to data privacy and security. The home study will be completed by all field staff prior to attending training; home studies will be graded and Interviewers will be required to correct items they miss.

- The FI training program will include comprehensive modules on data privacy and security. A certification station will involve completion of a certification exam on the key data privacy and security protocols for the survey. Interviewers must be certified before they can begin work.

- The FS training program will include comprehensive modules on data privacy and security, including compliance monitoring.

1.11 Information Provided to Respondents about Privacy

Within the informed consent document and in other verbal discussions of privacy, respondents are informed that their participation and the information they provide will be kept private. In addition, they are told that everyone involved in the study has signed an agreement stating they will protect the privacy of the information provided and that this information will not be shared with anyone at the health care center.

Detailed communication and reporting protocols will be developed for unanticipated situations in which the confidentiality of the respondent is compromised. The FI is required to immediately call the FS, who will immediately alert the Regional Supervisor. She will then alert the Data Collection Task Leader and the Project Director, who in turn will alert the client and RTI's Institutional Review Board (IRB). An adverse event report is prepared by RTI and submitted to RTI's IRB. This report describes in detail the problem that occurred, the estimated disclosure risk, the persons affected, when and where the problem occurred, and when project staff alerted RTI's IRB.