# Appendix V

# CATI Data Security Plan

This document describes the security features of the Research Triangle Institute (RTI) network in general and the PRAMS CATI architecture. PRAMS CATI has two major components, Web-based Case Management System (Web-CMS) and Web-based Interview (WI). Both the Web-CMS and WI will be housed on the RTI servers through September 2009. After that, CDC will contract with RTI or some other contractor to house the Web-CMS and WI systems or house them at CDC. In the event of a change in contractors or location, this appendix will be updated to reflect the new location's security plan.

## 1. PRAMS CATI Security

All PRAMS data will be stored and accessed in accordance with industry standard procedures. This includes username/password authentication to enter the PRAMS portal. User credentials will define their access level, allowing states to access ONLY their data. More stringent security will be imposed on the case management system participant identification table. This table will be accessible only through the state CMS view to facilitate case selection and contact. Response data will be maintained in a separate table containing no identifiers other than the case id. The system management console will provide a feature for state supervisory staff to export response data to tables for access by CDC once data entry for a batch is completed. However, CDC will not be able to access any tables until the state grants access. At no time will CDC PRAMS staff have access to the participant identification table.

- Participant Identification Table - This table will contain at least the case id for each participant. Based upon state agreement to transfer individual identification information this table may also include the following:
    - Participant name
    - Participant address
    - Participant phone numbers
    - Participant birth date
    - Other information relevant to the interview when applicable (infant death status, minor, Hispanic, multiple birth, etc)

  The table will be accessible only by system administrators and by the Web-CMS for validation of the participant's identity. For states who do not permit the transfer of individual identification information to Web-CMS, only the case id will be transferred. Interviewers will have to use face sheets with the

contact information generated by PRAMTrac in conjuction with Web-CATI to keep track of the correct participant and conduct the interviews.

- Question response table
    - Caseid
    - Question response values
    - NO participant identifying information

Data will be housed on RTI's servers in the RTI computing center managed by RTI's Information Technology Services division. RTI follows industry standard procedures for securing the computers, servers and networks physically and electronically.

The computing center is housed in a masonry building with automatic steel doors that are always locked. Physical access to the computing center is restricted to authorized personnel using card-key access. Fire protection is provided by a halon system.

RTI's networks are protected by an internet firewall that requires all of the traffic to pass through a single connection point and thus providing the maximum security possible without restricting legitimate access. Electronic access is restricted by the use of username and password access to authorized personnel only. Passwords need to be of certain minimum length, and has to have combination of alphanumeric and special characters and are changed on a periodic basis.

All network and computer systems in the computer room have Uninterruptable Power Supplies (UPS). These ensure continuous service during brief electrical power disruptions and minimize hardware failures. A diesel generator is available, to provide continuous operations during more extended power failures.

All Web interfaces to the project data will employ secure sockets layer security. This means that no clear text will move between client and server.

## 2. PRAMS Web-CATI Data Storage Protocol

As mentioned earlier, PRAMS CATI has two main components, the Web-CMS and WI. The Web-CMS will contain the personal identifiers to assist with identifying the appropriate mother. The WI on the other hand, will contain the survey responses but will only have a case ID number and will not contain any identifying data. The Web-CMS and WI will be housed in separate databases. Furthermore, data from a monthly batch will reside on Web-CMS and/or WI only for a limited amount of time, until the survey data for that batch have been cleaned and validated by the states and CDC.

The following provides a chronological outline of PRAMS CATI:

- As a batch goes into phone phase, appropriate locating information from PRAMTrac will be uploaded to the Web-CMS. If a state wants to utilize the CATI system to enter “call-in” interviews during the mail phase, they might choose to load the cases at an earlier point in time. Otherwise, those interviews will have to be recorded on paper for later data entry.
- Using Web-CMS, the CATI interviewers from the states will contact the mothers and complete the CATI interviews.
- Using Web-CMS, the states staff can perform the following:
    - Edit or update the data at any time to include new phone numbers or locating information.
    - Record final dispositions (hard refusal, completion, language barrier, etc).
    - Follow up cases that require further action (no answer, disconnected number, will mail, wrong number, appointment, etc).
- In addition, the PRAMS-CATI will do the following:
    - Synchronize the disposition codes with PRAMTrac on a periodic basis (nightly basis, if desired).
    - Provide standardized summary status reports that provide a snapshot of progress of phone phase.
    - Provide CATI scheduler reports that help in managing the cases to be called.
- State PRAMS staff can review and edit the survey data on a case by case basis.
- Once a batch is finished with phone phase, state PRAMS staff will export the call history and other phone operations data from CMS to PRAMTrac indexed only by the case ID (the data is only removed when the batch is deleted by the administrator ).
- Compare reports will be run by the states reviewing both mail and phone survey data (this step will occur outside of Web-CATI).
- After all of the interview records for the batch in WI have been cleaned and reviewed for completeness, the states will forward the phone interview file to CDC (it has not yet been determined whether this step will be done directly from the RTI servers or whether the file will be downloaded by the states and submitted over the Secure Data Network (SDN) along with the other data files for the batch). The Web-CATI system will not forward any interview data to CDC until authorization is given by the appropriate state staff.
- Once the batch has been submitted to CDC, phone interview data will remain on WI and accessible for further cleaning and editing based on the CDC batch submission error reports. Updates at this point to phone operations data will occur in PRAMTrac.
- Once CDC notifies that all data for the batch has been received and there are no errors to report, the state PRAMS staff will download all of the phone interview data for the batch to the states’ computers and instruct Web-CATI to

remove the monthly batch of records from the WI. After this point, there will be no records for that batch on RTI's servers.

Two levels of state users will be defined, supervisors and interviewers. Interviewers will have access only to those functions necessary to conduct the interview and review the interview data. Supervisors will have full access to Web-CATI functions including file upload/download, report generation, and removing batches from Web-CATI.

## 3. RTI Computing Network and Security

### A. Windows Network

#### i. Windows Server Built-in Security Features

Microsoft's Windows Server operating system family supports several security features, which include the following:

- Local desktop security: user identification and password required for access.
- Lockout of account upon repeated entry of an invalid password.
- NT File System (NTFS) per-file and per-directory security.
- Administrator-defined user groups.

NTFS permissions allow users and administrators to control access to NT resources on a per-user or per-user-group basis. NTFS has many levels of access control, including no access, read only, change, and full control.

#### ii. Password Control

Password management is critical to maintain computer and network security. RTI has taken appropriate measures to ensure that staff follow appropriate procedures. Every username (i.e., account) on all ITS systems has an associated password. No written or electronic record of passwords is generated. Automated controls are in place to ensure password quality (requiring a minimum length and a mix of uppercase, lowercase, numerals, and punctuation) and automatic periodic expiration of passwords.

#### iii. Backups

Under normal operating conditions, a complete backup of all files on every disk is written to tape weekly. Every business day, a differential backup is performed of all files created or modified since the last complete backup. In the event of a hardware or software failure, files can be restored to their status as of the time of the last differential backup, usually the evening of the previous business day. Tapes from complete backups are kept for approximately 3 months. Tapes or CD-R drives are used for long-term data archiving.

The tapes from the current complete backup are stored in the computer room for easy access. The tapes from the previous backup set are stored off-site. This procedure ensures data availability in the event of a catastrophic event in the computer room. The off-site company is a division of Brambles, a global leader in support services. Our Quality Assurance Regulatory Affairs (QARA) group conducted a facility evaluation and noted that the physical and logical security was both in place and well documented along with fire suppression, temperature, and humidity controls.

#### iv. Access by Non-RTI Staff

Users of RTI's facilities are primarily RTI employees. Some RTI contracts require that subcontractor or contracting agency staff have access to RTI's facilities. These users must follow the same policies and operating procedures as RTI staff, which specify that an appropriate level of approval must be gained before access is permitted.

### B. RTI Data Network

The RTI Data Network is a fully switched Ethernet-based network interconnecting all buildings on RTI's main campus as well as several remote locations. Buildings and servers in RTP are connected via Gigabit or Fast Ethernet (100 Mbps).

Remote offices are connected to the network via dedicated network circuits or via the Internet using Virtual Private Networks (VPNs).

Remote locations directly connected to the RTI network include downtown Washington, DC; Rockville, MD; Atlanta, GA; Chicago, IL; Waltham, MA; and three local facilities in the RTP area.

Remote locations provided access to the RTI network via VPNs include Cocoa Beach, FL; Hampton, VA; Manchester, UK; Philadelphia, PA; and Kiev, Ukraine.

RTI is connected to the Internet via a DS3 45 Mbps connection. A 6.2 Mbps backup connection ensures uninterrupted Internet connectivity.

The core of the RTI network is located in the computer room described below in **Section C.ii**. This ensures that the same level of physical security, electrical power conditioning, environmental conditioning, and monitoring is provided to the network equipment as to the servers. The network is automatically monitored for utilization and faults. Notifications are sent via e-mail and pager to the network on-call staff if a problem is detected.

#### i. Remote Access

The RTI network is accessible from remote locations in a variety of ways. V.90, V.34, and ISDN dial-in is available. The network supports PPP (Point-to-Point

Protocol) for remote network connections and Telnet and SSH for terminal emulation. Both local and toll-free numbers are available. Local numbers are available in Research Triangle Park, NC, and Washington, DC. User authentication (username and password) is required for all remote access to the network.

Access from the Internet is available to authorized staff but is controlled by RTI's Internet firewall (**see Section B.ii below**). VPN software is used to authenticate the user's identity and to encrypt communication between remote staff and the RTI network.

### ii. 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 the same level of protection and monitoring to all systems connected to or accessing 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 allow or prevent 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 is used to create two RTI networks with different levels of access from the Internet. These networks are called the "private network" and the "public network." The private network is the main RTI network, and most systems are located on it. Access to this network from the Internet is very limited, using a limited set of protocols into specific systems. For example, incoming electronic mail is only permitted to specific mail servers. The public network is more accessible from the Internet and is where World Wide Web servers, anonymous FTP servers, and other publicly available systems are located. Servers on the public network must be registered with ITS and must specify which services they run. This enables the firewall rules to allow only those services required. By not allowing unnecessary services, the overall security of the public servers is improved.

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 public network. Only approved file types are allowed on the web servers. For example, CGI scripts are not permitted on web servers.

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 are 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. This includes CERT, Microsoft, Network Associates, Trend Micro, and SANS. RTI is an active member in InfraGard, a cooperative security program between the FBI and commercial enterprises.

A multilayered anti-virus program is in place. All e-mail is scanned. Anti-spam filters are in place.

Security awareness articles are posted on the internal RTI Web site several times a year to ensure that staff remain aware and vigilant about following appropriate security precautions.

The Director of IT Security maintains an active Certified Information Systems Security Professional (CISSP) certification. The firewall administrator has been certified as an administrator by the firewall vendor.

#### iii. Voice over Internet Protocol

RTI has implemented a Voice over Internet Protocol (VOIP) system for the Call Centers. This system supports incoming call routing and interactive voice response (IVR). Redundant IVR servers, IP-PBXs, and voice gateways are utilized to ensure availability and adequate capacity. The VOIP system is connected to the main RTI voice network (telephone), ensuring full access to telephony resources from either the VOIP system or the traditional TDM PBX. This system was implemented following FDA guidelines for electronic technology, ensuring that planning, installation, modifications, and maintenance are fully documented.

### C. Physical Facilities

#### i. Buildings

RTI has installed a keyless card-controlled access system on all buildings and laboratories on RTI's main campus. Access is controlled 24 hours a day, seven days a week. The system monitors and limits access to the buildings and to the ITS computer room. Access is granted on an individual basis, and reports can be generated to review access patterns.

RTI security officers patrol the campus, confirm that the exterior doors to the buildings are locked, and walk through the buildings. Additionally, security officers inspect the ITS computer room for signs of unauthorized entry or access. Internal building checks are verified independently using a system that collects data from bar codes that are scanned using micro-wands. The data are loaded into a PC for review, analysis, and storage.

RTI has a radio/telephone system that allows immediate communication with RTI Security staff in emergencies.

All full-time Security staff are cleared by the Department of Defense and cleared for access to confidential business information (CBI).

### ii. Computer Room

The main computer room is located on RTI's main campus. The computer room is constructed of masonry and is secured by two automatically locking steel doors that are locked at all times.

Fire protection is provided by a halon system. If a problem is detected, automatic telephone dialers notify RTI Security and Maintenance, alarms sound, strobe lights flash, and the building-wide alarm is activated. There are override and emergency discharge switches for the Halon system in the computer room. ITS staff receive annual training in the operation of the halon systems and in emergency procedures.

Air conditioning and ventilation are provided in the computer room by two Liebert air conditioning systems, each sufficient to independently maintain an appropriate operating environment. Each Liebert system has built-in redundant compressors. The systems are separate from the heating, ventilation, and air conditioning systems in the parent building. Both temperature and humidity are monitored and alarmed. There are alarms to detect water under the raised floor of the computer room. Alarms are automatically transmitted to RTI Security and RTI Facilities and Maintenance staff 24 hours a day, 7 days a week via radio.

Continuous electrical service for the computer room is ensured by an uninterruptible power supply (UPS) and a diesel generator. The UPS ensures continuous service during brief electrical power disruptions and conditions the electrical supply minimizing hardware failures. The generator will begin function within seconds of a loss of utility company power. It provides continuous operations during more extended power failures. A 7-day supply of diesel fuel is maintained.

### iii. Visitors

Visitors are permitted in the computer room only when escorted by ITS staff. All escorted access to the computer room is recorded.