Attachment 6

Additional backup material

i. NORC protocol for physical and network security
ii. Detailed description of the locating process & database
iii. Description of the program & process used for web data collection
iv. Selected persons involved in developing SATH content and procedures

Attachment 6i.

NORC protocol for physical and network security

Physical Security/Facilities

NORC enforces a variety of physical security measures across all facilities, and ensure that access to all confidential data are restricted to only those employees that posses both the need and proper authorization to review such information. A keycard, key access, or human monitoring system (often times a combination of one or more may be used) restricts access to every facility.

- All server rooms, wiring closets, and network ports on the Wide Area Network (WAN) (with the exception of dial-up users) are located behind locked doors within the boundaries of a secure area inside the facility with restricted access to designated persons.
- All data collection and processing sites are located in restricted areas that are readily protected by either security systems, including video cameras and the aforementioned keycard systems or human monitors.
- Project-specific servers protect data and data access, which is only granted to members of project teams by Information Technology (IT) staff. The IT staff also maintains locked and secured filing and data storage facilities, and each of the project-specific, password-protected portal sites.
- Individually identifiable data on hard copy documents is captured electronically, separated from the questionnaire, and disposed of in accordance with project-specific instructions. When physical copies must be retained or are not in use, they are stored in locked file cabinets that are accessible only to authorized project staff.

Network Data Security

Internal network storage is provided for each project to mitigate the potential of data loss due to accidents, computer equipment malfunction, failure, or human error; and to administer access rights.

- Production file servers are equipped with fault tolerant disk arrays and redundant power supplies to minimize the risk of losing valuable project data. These data are protected by surge suppression and Uninterruptible Power Supplies (UPS).
- All operating system vendors are routinely monitored by a designated IT infrastructure resource monitor for security patches with all updates applied as necessary. Data

transfers to removable media for purposes of client delivery or archival is performed by the IT department to control data formatting and provide assurance that the media is readable by the client. This also gives the IT department the opportunity to scan the deliverables for viruses while maintaining detailed shipping manifests and receipts of all deliveries.

- All authorized network users are issued a user-id and password which must be used to sign into each of the project applications and data areas located on the network. Employees are required to change their server passwords on a regular basis.
- The installation of any software package on a computer is controlled, and requires successful completion of a through software review and approval process.
- Remote access into the network is performed through NORC's firewall using a Virtual Private Network (VPN). A firewall and a packet filtering router have been set to protect each NORC Internet Access Point, and a designated NORC IT infrastructure resource is employed to monitor the Local Area Network (LAN) and WAN for signs of intrusion and other security violations. Host-based applications such as FTP and web servers are run only on servers inside the data center, and are separate from servers designated to store and collect client data.
- Connectivity between all sites is protected by dedicated data circuits. Any data that are placed on any public networks is encrypted. There is also a dedicated IT resource to maintain a software package that proactively searches for security holes and recommends fixes in a timely manner.
- NORC routinely engages third-parties to conduct network security audits, which includes comprehensive attempts at network penetration from undisclosed sources and a review of policies and procedures.

Application Security

All applications that manage case, response, and corporate financial data protect against unauthorized access and restrict authorized access to the minimum necessary level.

User Rights

Once logged into the application system, each user-id is assigned a 'rights mask' that allows the user access only to limited views of data.

Case-Level Security

Unique case identifiers are used to create a partition between response data, and data that could be used to identify an individual.

Encryption Key Management

All applications used in any environment outside of the WAN are required to use digital certificates that encrypt data using Secure Sockets Layer (SSL) technology (where applicable).

Electronic Data Transfer External to NORC

Should a project obligation require that data be electronically transmitted to or from the secure private network, encryption technology will be used.

Access Control / Authentication

All attempts to access data are logged by the hosting server for review.

Employee Exit

Human Resources (HR) and IT coordinate so that user accounts are deactivated upon employee exit. An exit interview checklist of security-related steps is utilized by both HR and IT.

Backup Procedures

All data that currently reside on the network is backed up on tape on a nightly basis. These tapes are stored in a secure, off-site location. Any information housed on these tapes is retrievable from the storage facility within 12 hours. All backups made for the purpose of disaster recovery have a retention period of one year. At the conclusion of a project, an archive is immediately created in strict accordance with contractual requirements. All archived project materials are stored off-site and easily accessible to staff.

Data Retrieval

Only a limited number of IT personnel are authorized to request the retrieval of these data tapes from the off-site location, and must follow an identification and authorization procedure.

Virus Protection

All systems are protected from computer viruses by extremely robust security features and procedures.

The technique of limiting user access to internal network data storage is designed specifically to minimize the possible impact of a virus that may breach virus protection software and procedures. Several actions are taken on a daily basis to prevent a virus from breaching the system.

- Virus scans are completed routinely through the use of commercially available and automatically updated software.
- Employee workstations are configured to automatically check all files that are used, including those coming from diskettes and email attachments, to ensure that they are not introducing viruses to the system.

- Incoming email attachments are automatically screened on the email server for viruses, Trojan Horses, worms, and related malignant software.

Paper Records Storage and Security

Business records are kept to meet operating, historical, research, audit, and legal requirements. Records are only destroyed at the appropriate time.

Temporary Storage

Secured, general storage is referred to as the 'cold storage area'. Any materials without respondent identifiers may be stored in cold storage to be easily accessible to project personnel. This space also serves as a staging area to access and inventory materials for permanent archiving. Paper files pertaining to project management are separated from production data and stored permanently at this location.

There are two locked "cages" available. Access is restricted to the records manager or librarian. All sensitive contracts, grants, personnel, and financial records are kept in one of these secure double locked areas.

Materials are stored in acid free cartons and are labeled with the project name and number, project supervisor name and telephone number, and projected destruction date. A list of contents for each box sent for storage must be provided, and materials will not be disposed of without contacting the appropriate personnel. Before storing hard copy survey materials, cartons are inventoried and contents are recorded. Requests for stored items are made to the records manager.

Long-Term Storage

Project directors may request that materials be stored on a more permanent basis at a remote storage area, and fulfills contractual obligations of records storage when limited access to records is required. We currently have a contract with O'Hare Record Retention Company (ORRC) in Cicero, Illinois. This facility has a sophisticated sprinkler system and a NORC-approved disaster plan in place. General access to the facility is limited to the records manager and NORC librarian. Should a site visit be required by either NORC personnel or our clients, we must provide the records manager at least 24 hours notice and submit a list of the planned visitors. ORRC requires that visitors provide proper identification and be accompanied by either the records manager or librarian. Space at the facility for the examination of materials is available for a reasonable fee.

All materials are inventoried and receive unique bar codes as identifiers before being delivered to ORRC, and a copy of the inventory is kept on the shared drive. Production materials may be sent directly to ORRC.

Attachment 6ii.

2007 SATH:
Detailed description of the locating process & database

Description of the database used in the locating process

Accurint is owned by LexisNexis (LN) which provides comprehensive and authoritative legal, public record, news, and business information and tailored applications, will be used to conduct the locating effort. LN does not collect personal financial, credit, or medical information.

The Accurint database is a widely used 'locate-and-research' tool and allow users to locate persons; track down telephone numbers with access to over 50,000,000 non-directory assistance records (including cellular telephone numbers); link over 132 million individuals to businesses and business contact information based on probable current and historical employment information; and includes a search tool to help find individuals when only old or fragmented data are available. This database is used by NORC to track participants in large nationally-representative longitudinal surveys such as the National Longitudinal Survey of Youth (NLSY) sponsored by the Bureau of Labor Statistics (BLS). Locators will enter the 2001 telephone number into the online Accurint system and obtain some level of information.

Description of the batch locating process

NORC will use Accurint for batch locating. For the SATH, NORC will have very limited information to start with. Using a batch submission, NORC will request a list of current household members as well as household members from 2001. This information from Accurint will be pre-loaded into the locating or Case Management System (CMS) as 'leads' (these systems are integrated). If a lead for each case does not turn into either a 2001 and/or 2007 contact, the case will re-enter the locating system. Incorrect contacts determined during CATI screening will also reenter the locating system. During this locating process NORC will use an unscripted approach to initially contact the household to locate the 2001 respondent. It would be impossible to write appropriate scripts that will address every possible scenario the locators will face when 'cold calling' the 2001 telephone numbers. When the eligible cases are located, interviewers will use a traditional scripted approach to recruit the case and give informed consent information.

The CMS has the ability to email or mail project information to respondents by case disposition codes. Eligible cases can be easily and efficiently flagged if they request information. Within the locating procedure, all 'finalized' cases go to the locating supervisors who assign disposition codes.

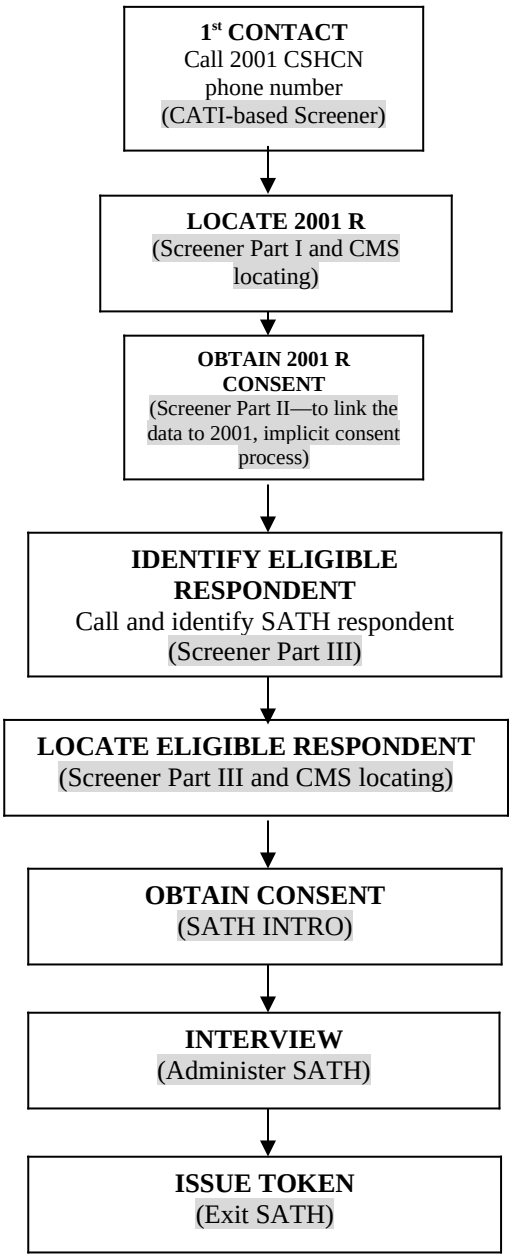
Once all telephone options to locate the case are exhausted, further searches will occur using the internet. These 'web treatments' will include the use of commonly available search engines such as Java Search and Google. These resources will only be used when needed, and certain components will be entered only by supervisors.

The children who in 2001 were receiving all the necessary transition services are a minority of cases but because of their importance to this study, they will receive more intensive locating protocol. They are considered "imperative" cases while all others are considered "standard" cases. Standard cases that cannot be located will be re-released to the locating staff for continued attempts to locate until the end of data collection. All locators are highly trained interviewers and are able to seamlessly segue into the 2007 interview if the proper person is located, is immediately available, and gives consent. Incorporated into the scripts and procedures is a recognition of the passage of time as well as the portability of telephone numbers in the interim period.

Training will clearly stipulate what criteria are authorized for search. Locators will also be thoroughly trained in what they are and are not allowed to tell people who may not be the intended household or respondent but answer their calls.

Only previously successful, professional, and very experienced locators and interviewers will be assigned to this project. Although we will encourage all respondents to respond via a landline phone or website, we will attempt to conduct the interview using a cellular phone if this is the only option.

The figure below summarizes the general process flow for the 2007 SATH. The shaded words in the boxes refer to either the position within the locating or interviewing process, or the relevant instrument scripts or sections.



Attachment 6iii.

2007 SATH:
Description of the program & process used for web data collection

A web-based internet application has been developed to collect data in lieu of the traditional computer-assisted telephone interviewing (CATI) program that we have used consistently for other modules. It allows us to streamline instrument development and reduce the amount of preparation time because only one version of the survey will need to be constructed regardless of mode, instead of having to construct a CATI-version and a web version.

Specifically, NORC will extend the functionality of the CATI data collection program that is currently used to collect NIS/SLAITS data. This program has an option that allows it to capture data entry over the web. A web server will securely deliver content to the respondent. All questionnaire data (CATI and web) can be collected into one integrated data store for analysis.

For respondents who choose to complete the interview over the telephone, the identical web-based program will be used to collect the data; however, the interviewer will read the question over the telephone to the respondent and enter the response. The computer program guides the interviewer (or respondent) through the questionnaire (question by question and page by page), automatically routing the interviewer (or respondent) to appropriate questions based on answers to previous questions. The CATI program determines if a selected response is within an acceptable range, checks entry for consistency against other data collected during the interview, and saves the responses into a survey data file. On-line help menus are also available. This data collection technology reduces the time required for transferring, processing, and releasing data.

Should a phone or web interview terminate before completion, the system allows the interviewer or respondent to resume at the break-off point at another time. Because of multiple administration modes, the instrument was simplified as much as possible to minimize confusion (very few skip patterns, et cetera).

For interviews conducted using a telephone this system documents all call attempts and the outcome of each, their time and duration, and schedules future calls. Further, it documents if and when a message should be left on the household's answering machine or voice mail. The system assigns calls to interviewers and dials the numbers, although cellular phone numbers will be hand-dialed.

We will format the questions and screens by incorporating the most up-to-date research[1] (i.e., the screen text may not appear exactly as listed below).

The screen in the secure data collection environment will display the following text:

> ***The Centers for Disease Control and Prevention (CDC) is doing a nationwide survey about the health of young adults, and their health status and health care as they get older. In 2001, we spoke to someone in your household about health care. The CDC would like to examine changes that may have occurred in your health or healthcare in the past few years by getting information directly from you.***

[1] Dillman, Don A. *Mail and internet surveys: The Tailored Design Method, Second Edition (includes a 2007 update with new internet, visual, and mixed-mode guide)*. Hoboken, New Jersey: John Wiley & Sons; 2007.

It is your choice to participate in this research. You may choose not to answer any question you don't wish to answer--simply leave it blank. You may also choose to stop the survey at any time, or stop now and continue it at a later time. You will be able to restart the survey where you left off.

This study is authorized by the U.S. Public Health Service Act. This and other strict laws require us to protect your privacy and use your answers only for statistical research. You can see these laws by clicking here[2].

The survey will take about 15 minutes. In appreciation, you will receive $20. If you have any questions about this study, please call the study's toll-free number, xxx-xxx-xxxx.

The survey contains questions about your health, health status, and health care as you get older.

Instructions will explain the navigation process, and for persons who chose to complete the survey in stages, i.e., exit the program and return to complete the survey at a more convenient time. To confirm this is the correct respondent, he/she must confirm his/her date of birth. The instrument will then display question F2Q11 (i.e., the start of section 2, health and functional status).

When the respondent completes the web survey, the screen will display the following text:

Those are all the questions. Thank you for participating in the 2007 Survey of Adult Transition and Health. In appreciation for your time, we would like to send you 20 dollars.

Please enter your name and mailing address:

NAME_____
STREET_____
CITY_____
STATE _____
ZIP _____

We'd like to thank you on behalf of the Centers for Disease Control and Prevention for the time and effort you've spent answering these questions. If you would like more information about this survey, please

---

[2] This link will lead to a screen that will display the following information:
Federal laws guarantee that your answers will be used only for statistical research. The Public Health Service Act is Volume 42 of the US Code, Section 242k. The collection of information in this survey is authorized by Section 306 of this Act. The confidentiality of your responses is assured by Section 308d of this Act and by the Confidential Information Protection and Statistical Efficiency Act.

call the study's toll-free number, xxx-xxx-xxxx. If you have questions about your rights as a study participant, you may call 1-800-223-8118, toll-free, and leave a message asking to speak to the Chairperson of the Research Ethics Review Board. Again, thank you!

Attachment 6iv.

Selected persons involved in developing SATH content and procedures

LISTED ALPHABETICALLY BY LAST NAME

Stephen Blumberg, Ph.D.
Senior Scientist
Centers for Disease Control and Prevention
Hyattsville, MD
sblumberg@cdc.gov

Matthew Bramlett, Ph.D.
Survey Statistician
Centers for Disease Control and Prevention
Hyattsville, MD
mbramlett@cdc.gov

Marcie Cynamon, MA
Chief, Survey Planning and Special Surveys Branch
Centers for Disease Control and Prevention
Hyattsville, MD
mcynamon@cdc.gov

Michael Kogan, Ph.D.
Director, Office of Data and Information Management
Health Resources and Services Administration
Rockville, MD
mkogan@hrsa.gov

Julian Luke, B.A.
Lead Computer Scientist
Centers for Disease Control and Prevention
Hyattsville, MD
jluke@cdc.gov

Paul Newacheck, Dr.P.H.
Professor of Health Policy
Institute for Health Policy Studies
University of California, San Francisco
San Francisco, CA
pauln@itsa.ucsf.edu

Kathleen S. O'Connor, M.P.H. (CDC team leader)
Survey Statistician
Centers for Disease Control and Prevention
Hyattsville, MD
koconnor1@cdc.gov

Bonnie Strickland, Ph.D.
Acting Director, Division of Services for Children with Special Health Care Needs
Health Resources and Services Administration
Rockville, MD
bstrickland@hrsa.gov

Peter van Dyck, MD, MPH
Associate Administrator
Health Resources and Services Administration
Rockville, MD
pvandyck@hrsa.gov