

Attachment A
Form to Describe Sensitive Data Security Plan
For the Use of Sensitive Data from
The National Longitudinal Study of Adolescent to Adult Health

Data Stored on a Server

All requests for data must include the following information.

I. General Information

1. List below the name(s) and responsibilities of the investigator(s) and the research staff (students, research assistants, and programmers) who will have access to the data. Changes in personnel require that this information be updated.

Lauren Gaydosh (PI), Aanchal Bagga (research assistant), Katrina Tsun (research assistant)

1b. PI Institution

PI contact information: Email: lauren.m.gaydosh@vanderbilt.edu

Phone number: 615 343 7683

System Administrator contact information: Name: Todd Dodson

Email: todd.dodson@vanderbilt.edu

Phone number: 6153434129

2. Each project participant must sign a separate security pledge to be included with the contract. As new personnel are added during the period of this contract an amended Attachment C and new security pledges must be obtained and sent to the Carolina Population Center. A security pledge form can be found under Attachment D. Please copy for each participant.

Number of security pledges included: 3

3. Only one complete copy of the Add Health data is permitted; however, time-delimited temporary data analysis files may be created. Temporary data analysis file(s) must be deleted every six months and recreated, as necessary, to complete analysis. Temporary data analysis files should be deleted upon completion of a project.

All temporary data analysis files will be deleted January and June every year.
month month

4. Add Health data, including temporary data analysis files or subsets of the data, may not be copied to other media such as CDs or diskettes or downloaded to other platforms or machines. All Add Health data must remain in the same secure location as the one copy of the original Add Health data.

LG I agree to this condition.
Investigator initial

II. Detailed description of computer system where data will be stored and analyzed

1. Please select the type of server/operating system you will be using:

- ☐ Windows File Server OS Version: _____
- ☐ Windows Terminal Server OS Version: _____
- ☐ Linux Computing Server Version: _____
- ☐ Linux SAMBA File Server Version: _____
- ☒ SAN Product/Version: **Dell EMC Isilon**

2. What is the **physical location** of the server hardware?

Street Address	1231 18th Ave. South Nashville, TN 37212
Building	Hill Center
Room #	148

3. What is the **physical location(s)** of the end user's computer(s)?

Street Address	
Building	Calhoun Hall
Room #	Suite 300 Office 321

4. How will Add Health data be excluded from the backup routine, *if not using an enterprise backup environment* (specified below)?

- Enter "Y" if you are using the specified backup solution
 -- Enter "N" if you are not using the specified backup solution

Y	Enterprise-level Server backup/archive: <i>Server Replication</i> ADD Health Data specially excluded.
Y	Enterprise-level Server backup/archive: <i>Snapshots</i> Snapshots viable only to authorized to primary data
N	Enterprise-level Server backup/archive: <i>Tape backup (must be encrypted)</i>
N	Enterprise-level Server backup/archive: <i>Other, Specify:</i>
<input checked="" type="checkbox"/>	By checking this box, I verify that Add Health data is not being backed up
<input type="checkbox"/>	By checking this box, I understand that I may and should back up my program code and documentation, as described below

5. Who has physical access to the server equipment?

Members of the Data Center Services team have access to the data center with card and fingerprint access. The Data Center Services team are the only ones with keys to the server racks.

6. Who has permission to use the server equipment?

Professionally Administered by VUIT Storage. Storage team creates shared and delegates access to local support. Each share partitioned from others. Only people with access to share have permissions to use/see data.

7. Is the server equipment used by other projects?

Yes. Used by multiple groups but shares are segmented. Access controlled by security groups and only authorized users can access this data.

8. Where will hard copy info be printed?

Calhoun Hall, Suite 300

9. How will hard copy data be handled/stored/discarded?

X	All printed copies of data output will be contained in a labeled folder
X	When not in use, paper copies will be stored in a locked filing cabinet
X	When researchers are no longer using the printouts, they will be shredded
Other, Specify:	

10. What is the secure storage location of the original data CD?

Street Address	
Building	Calhoun Hall
Room #	Suite 300 Office 321
Storage Unit	Locked file cabinet

11. I will not copy or move the Add Health data out of the secured directory or off of the secured server for any reason.

LG

I agree to this condition.

Investigator initial

III. Server Security Protocols:

Complete the following table to indicate which security protocols are in place in the server environment.

- Place a "Y" next to the protocols that are being implemented.
- Place an "N" next to the protocols that are **not** being implemented.

Internet Filtering [special router ACLs or campus firewall]	Y
Campus Filtering [vlan ACLs or firewall]	Y
Host-Based Firewall	Y
Intrusion Prevention System (e.g., Tipping Point)	Palo Alto
Managed and Monitored Malware Protection: <i>Name/Version:</i>	CrowdStrike EDR
Detailed Auditing for Access (account access)	N
Detailed Auditing for Access to all Sensitive Files (file access)	N
Local System Event Logs	Y

Remote Copy of System Event Logs	Y
24/7 Monitoring (ping monitoring to ensure availability)	Y
Authenticated Operating System Vulnerability Scans (e.g., QualysGuard)	Y
Password Policy Enforcement (User and Administrator)	Y
Multi-Factor Authentication	N
Encryption (File/Folder or Partition for all SI)	N
Least Functionality (i.e., installing only needed services. e.g., not IIS or SQL)	Y
Least Privilege (refers to user accounts, service accounts, and processes)	Y
Secure Physical Access	Y
Patch Management (Automated Recommended)	Y
IT staff configuring and maintaining system	Y
IT Security Awareness for End Users (e.g., NIH example, http://irtsectraining.nih.gov/CSA/0000000.aspx)	Y
Warning Banner for Services Requiring Authentication	Y
System's Administrator's Contact Info: <i>Lane Williams 615-715-9987</i>	Y
Risk Assessment	Y
Vendor-Supported Operating System (e.g., still getting patched/updated by vendor)	Y
Vendor-Supported Applications (e.g., still getting patched/updated by vendor)	Y

IV. Workstation Security Protocols

Complete the following table to indicate which security protocols are in place on the user's computer from which they connect to the server.

If you are using a **Linux SAMBA Server, Windows File Server or SAN**, it is especially important to keep the data off the local computers (e.g., redirecting temp files back to the server share), and ensure security on the local computers, so keep that in mind when implementing security protocols on the local computers.


- Place a "Y" next to the protocols that are being implemented.
- Place an "N" next to the protocols that are *not* being implemented.

Central Campus IT: Internet Filtering [special router ACLs or campus firewall]	Y
Central Campus IT Filtering (from other hosts) [vlan ACLs or firewall]	Y
Central Campus IT: Intrusion Prevention System	Y
Host-Based Firewall	Y
Use a managed and monitored Antivirus/Malware protection software (e.g., Symantec antivirus, SCEP, https://www.clamxav.com/)	CrowdStrike
Detailed Auditing for Logon success/failures	Y
Detailed Auditing for Access to all Sensitive Files	N
Local system event logs	Y
Operating System Vulnerability Scans: Authenticated (e.g., QualysGuard)	N
Require userid/strong password to login (do not use autologin)	Y

Password Policy Enforcement (Strong password changed periodically)	Y
Full-Disk Encryption (e.g., PGP Whole Disk Encryption, Bitlocker or FileVault) Specify: <u>FileVault</u>	Y
File/Folder/Partition Encryption (e.g., EFS, VeraCrypt, etc.). Specify: _____	N
Employ "Least Privilege." (e.g., don't login as local admin/super user)	N
Physical security: <input checked="" type="checkbox"/> locked office or _____ locking cable attached to desk	Y
Patch Management (Automated Recommended) Specify: <u>Updates pushed via AirWatch (Workspace ONE)</u>	Y
VPN Software for remote access (If connecting while off-campus, please complete a remote access form)	Y
IT Security Awareness for End Users (e.g., NIH example, http://irtsectraining.nih.gov/CSA/0000000.aspx)	Y
Vendor-Supported Operating System (e.g., still getting patched/updated by vendor) Specify: <u>Mac OS 10.14.3</u>	Y
Vendor-Supported Applications (e.g., still getting patched/updated by vendor)	Y
Redirect all temp files for the Add Health data back to the CIFS share (http://www.cpc.unc.edu/projects/addhealth/data/restricteduse/security/tempfiles)	Y
Screen Saver set to activate after 3 minutes of inactivity and screens locked whenever researchers leave their computers. If controlled by GPO at campus-level, and less than 3 minutes, specify screen saver activation time: _____	Y

List below or attach any additional security protocols at the end of this document.


Investigator initial


IT staff initial

