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 (by PI and SysAdmin)

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 by email to Add Health Contracts.

2. PI Institution: _____
3. PI contact information:

   Name: _____ Phone number: _____

   Email: _____

4. System Administrator ***(your IT professional)*** contact information:

   Name: _____ Phone number: _____

   Email: _____

5. Each project participant and system administrator 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 (Attachment D) must submitted to Add Health for approval before access is allowed.

   _____ I agree to this condition.
   PI initials

6. Each user accessing the Add Health data must submit section IV of this form and may need to submit sections VI and VII (see section V to determine whether this is required). Access will not be granted until the forms have been approved by Add Health.

   _____ I agree to this condition.
   PI initials

7. Only one complete copy of the Add Health data is permitted.
   – Users may create interim data analysis files and store them on the external hard drive.
   ("Interim" files are different from temp files created by statistical applications during sort/merge procedures.)
   – These interim data analysis file(s) must be deleted every six months and recreated to complete analysis.
   – Interim data analysis files must be deleted upon completion of a project.

   All interim data analysis files will be deleted in these two months each year:

   _____ and _____
   month *month*

8. Add Health data may not be copied to other media (including, but not limited to, CDs, flash drives, the hard drive of the computer, phone, or tablet). This includes interim data analysis files or subsets of the data. All Add Health data must remain in the same secure location as the one copy of the original Add Health data.

   _____ I agree to this condition.
   PI initials

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

Street Address	
Building & Room #	
Storage unit	

(e.g., locked drawer, or locked cabinet, or safe)

II. Detailed description of server system where data will be stored and Server Protocols (by SysAdmin)

10. Please specify the type of server/operating system you will be using.

Remote Compute options:

- ☐ Windows Terminal Server .....OS Version:..... _____
- ☐ Linux Compute Server .....Version:..... _____
- ☐ Virtual Desktop Infrastructure (VDI) .....Version: ..... _____

File Server options:

- ☐ Windows File Server .....OS Version:..... _____
- ☐ Linux SAMBA File Server .....Version:..... _____
- ☐ Other file server (e.g., Novell, Macintosh, NAS/SAN).....Appliance/Version: . _____

11. What is the physical location of the server hardware?

Street Address	
Building & Room #	

12. *We use an Enterprise environment*, and are backing up the Add Health data in the following ways:

____ Enterprise-level Server backup/archive: *Server Replication*

____ Enterprise-level Server backup/archive: *Snapshots*

____ Enterprise-level Server backup/archive: *Tape or disk backup (must be encrypted)*

____ Enterprise-level Server backup/archive: *Other, Specify:*

_____

13. *We are not using an Enterprise environment:*

_____ I verify that Add Health data is not being backed up.
SysAdmin initials

14. Server Security Protocols

Please tell us whether you are using the specified protocol…	**Y or N**
Internet Filtering *[special router ACLs or campus firewall]*	
Campus Filtering *[vlan ACLs or firewall]*	
Host-Based Firewall	
Intrusion Prevention System (e.g., Tipping Point)	
Managed and Monitored Malware Protection: *Name/Version:* _____	
Detailed Auditing for Access (account access)	
Detailed Auditing for Access to all Sensitive Files (file access)	
Local System Event Logs	
Remote Copy of System Event Logs	
24/7 Monitoring (ping monitoring to ensure availability)	
Authenticated Operating System Vulnerability Scans (e.g., QualysGuard)	
Password Policy Enforcement (User and Administrator)	
Multi-Factor Authentication	
Encryption (File/Folder or Partition for all SI)	
Least Functionality (i.e., installing only needed services. e.g., not IIS or SQL)	
Least Privilege (refers to user accounts, service accounts, and processes)	
Secure Physical Access	
IT staff configuring and maintaining system	
IT Security Awareness for End Users (e.g., NIH http://irtsectraining.nih.gov/CSA/0000000.aspx)	
Warning Banner for Services Requiring Authentication	
Risk Assessment	
Patch Management *Please specify:* _____ *(e.g., WSUS, SCCM)*	
Vendor-Supported Operating System is still new enough to be getting patched/updated by vendor *(Windows XP, for instance, is no longer supported)*	
Vendor-Supported Applications are still new enough to be getting patched/updated by vendor(s) (*Examples are SAS and Stata)*	

15. Additional security protocols are attached at the end of this document.

◯ Yes ◯ No

16. Who has physical access to the server equipment?

17. Who has permission to use the server equipment?

18. Is the server equipment used by other projects?

III. SysAdmin confirmations

_____ I acknowledge that I consulted with the Investigator (PI).
System Administrator initials

_____ I acknowledge that I completed these Server Security Protocols.
System Administrator initials

IV. Agreements by Researcher: _____ (by PI and each Researcher)

19. Add Health encourages you to back up your programming code and documentation so that you are able to recreate your interim analysis files in case of catastrophic computer failure.

    _____ I understand that I *may and should* back up my program code and documentation.
    user initials

    My backup procedure is: [ ]

20. Where will hard copy information be printed?

    [ ]

21. If you will print hard copy information, initial each of the following protocols to acknowledge your agreement.

    _____ All printed copies of data output will be contained in a labeled folder.
    user initials

    _____ When not in use, paper copies will be stored in a locked filing cabinet.
    user initials

    _____ When printouts are no longer being used by researchers, they will be shredded.
    user initials

22. If you will print hard copy information, describe how it will be handled/stored/discarded.

    [ ]

23. If the Add Health data is stored on a file server (refer to question #10 above or check with the contract investigator); your statistical applications must be configured to point the temporary working files back to the file server.

    Specify the drive and pathname of the temp directory: _____

24. I will not copy or move the Add Health data from the secured directory on the server for any reason or by any means.

    _____ I agree to this condition.
    user initials

V. Do you need to submit sections VI and VII? (by SysAdmin)

25. We are using a remote compute server to store the Add Health data.
    ◯ Correct ◯ No

26. Users must use multifactor authentication (MFA) to connect to the Remote Compute Server.
    ◯ Correct ◯ No

27. Printouts and/or downloads are either not permitted or are permitted if first vetted.
    ◯ Correct ◯ No

28. Please specify whether printouts and/or downloads are permitted:
    ◯ Not permitted ◯ Permitted if first vetted by the following persons

    _____ will do the vetting.

    _____ will oversee the printing.

    _____ will perform the downloads.

Skip sections VI and VII

- If CORRECT to all three protocols (questions 25, 26, 27):

Else:

- Submit section VI for each researcher (including PI).
- Submit section VII for each computer that wil be used.
  (If a computer will be used by more than one researcher, include their names on the form and submit just one copy).

VI. Workstation Description for Researcher(s): _____ (by PI and each researcher)

29. Please tell us about the computer you are using to access the Add Health data that is stored on the server:

    _____ _____ ◯ *laptop* ◯ *desktop*
    brand/make (e.g., Dell, Mac, etc.) *model (e.g., Optiplex, Dimension, iMac Pro, MacBook Air, etc.)*

30. Please tell us about the operating system (OS) you are using:

    _____
    version # and name of OS (Windows might be Home, Pro, Education, Enterprise; Mac might be Catalina, Mojave, High Sierra, etc.)

To find the Windows 10 "name"	To find the Mac OS "name"
Press the Windows key (⊞)+R, type "dxdiag" in the pop-up window, see "Operating System"	From the Apple menu (), choose About This Mac. see "macOS *****"

31. What is the physical location where you will be working when accessing the Add Health data?

Street Address	Building	Room #

VII. Workstation Security Protocols (by SysAdmin)

◯ These are the protocols for the following researchers who will use an institution-owned-and-maintained computer.
_____ _____ _____ _____ _____

◯ These are the protocols for researcher _____ who is using own computer.

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 (i.e., redirecting temp files back to the server share), and ensure security on the local computers.
- Please keep that in mind when implementing security protocols on the local computers.

Please tell us whether you are using the specified protocol…	**Y or N**
Central Campus IT: Internet Filtering (e.g., special router ACLs or campus firewall)	
Central Campus IT Filtering (from other hosts): (e.g., vlan ACLs or firewall)	
Central Campus IT: Intrusion Prevention System	
Host-Based Firewall	
Use a managed and monitored Antivirus/Malware protection software (e.g., Symantec antivirus, SCEP, https://www.clamxav.com/)	
Detailed Auditing for Logon success/failures	
Detailed Auditing for Access to all Sensitive Files	
Local system event logs	
Operating System Vulnerability Scans: Authenticated (e.g., QualysGuard)	
Require userid/strong password to login (do not use autologin)	
Password Policy Enforcement (strong password changed periodically)	
Full-Disk Encryption (e.g., PGP Whole Disk Encryption, Bitlocker or FileVault) *Specify:* _____	
Employ "Least Privilege." (i.e., don't login as local admin/super user)	
Physical security: *Specify:* _____ locked office _____ locking cable attached to desk	
Patch Management (Automated Recommended) *Specify:* _____	
VPN Software for remote access (If connecting while off-campus, please complete a remote access form)	
IT Security Awareness for End Users (e.g., NIH: http://irtsectraining.nih.gov/CSA/0000000.aspx)	
Vendor-Supported Operating System (i.e., still getting patched/updated by vendor) *Specify:* _____	
Vendor-Supported Applications (i.e., still getting patched/updated by vendor)	
Redirect all temp files for the Add Health data back to the CIFS share (Click here for how to redirect temp files) *(This protocol not applicable if using remote compute server.)*	
Screen Saver is set to activate after 7 minutes of inactivity ***and screen is locked whenever researcher leaves the computer***. If controlled by GPO at campus-level, and more than 7 minutes, specify screen saver activation time: _____	

System Administrator

_____ I acknowledge that I consulted with the user of this workstation.
System Administrator initials

_____ I acknowledge that I completed these Workstation Security Protocols.
System Administrator initials