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. Contact information:

   Required: PI Name: _____

   Phone number: _____ Email: _____

   Optional: person assisting PI Name: _____

   Phone number: _____ Email: _____

   Required: System Administrator ***(your IT professional)***: Name: _____

   Phone number: _____ Email: _____

4. 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 additional Attachment C and new security pledges (Attachment D) must submitted to Add Health and approved before access is allowed.

   _____ I will get approval for Att C and Att D for new users before granting access to the Add Health data.
   PI initials

5. Each user accessing the Add Health data must submit Section IV of this form (User Agreements) for review. Approval by Add Health is required before access is allowed.

   _____ I will get approval for Sect IV User Agreements for new users before granting access to the data.
   PI initials

6. Only one complete copy of the Add Health data is permitted.
   – Users may create interim data analysis files and store them on the server.
   (“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*

7. Add Health data may not be backed up.

   _____ I agree to this condition.
   PI initials

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. Renewing contracts only: What is the secure storage location of the original data CD(s)?

   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:

    Not available for new or renewing contracts

    Renewing contracts with previously approved File Server should contact Add Health Contracts (addhealth_contracts@unc.edu)

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., MECM)*	
Operating System is still being patched by vendor *(Windows 7, for instance, is no longer supported)*	
Applications are still being patched by vendor that developed application. (*Examples are SAS and Stata)*	
Screen Saver is set to activate after 10 minutes of inactivity.	

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: _____ (PI and each Researcher submits individually)
Name of user signing this copy of this section

19. Add Health encourages you to have a back-up of 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 my program code and documentation should be backed up.
    user initials

    _____ My program code and documentation are backed up on the server (if so, skip to Q20).
    user initials
    or NO

    _____ My program code and documentation are not backed up on the server; my backup procedure is:
    user initials

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 if differently than Q21.

23. 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 original Add Health data, interim data analysis files, and any other subsets of the data.

    The original Add Health data must remain in the **read-only directory** as approved in this Security Plan.

    Subsets of data (created by your researchers' programming code) must be stored in a separate directory on this same approved server.

    _____ I will not move any version of Add Health data from the secured directories on the server.
    user initials

    _____ I will not copy any version of Add Health data for any reason or by any means.
    user initials

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

24. Are you using a **Remote Compute Server** to store the Add Health data?
    - ☐ Yes, we are using a remote compute server to store the Add Health data. *[continue to Q25]*
    - ☐ No, we are not using a remote compute server *[skip to Section VI and submit Sections VI and VII]*

25. Are users required to use **multifactor authentication (MFA)** to connect to the Remote Compute Server?
    - ☐ Yes, users must use MFA to connect to the Remote Compute Server.. *[continue to Q26]*
    - ☐ No, users are not required to use MFA. *[skip to Section VI and submit Sections VI and VII]*

26. Are **printing and downloading** permitted?
    - ☐ No, printing and downloading are not permitted under any circumstances. *[skip the rest of this form]*
    - ☐ Yes, printing and downloading are permitted without restriction. *[skip to Section VI and submit Sections VI and VII]*
    - ☐ Printing and downloading will be permitted under these circumstances:

        26a. _____ will do the vetting. *[continue to 26b]*

        26b. _____ will oversee the printing. *[continue to 26c]*

        26c. _____ will perform the downloads. *[skip the rest of this form]*

VI. Workstation Description for Researcher(s): (PI and each researcher submits individually)

27. Researcher name(s): _____
    Name(s) of researcher(s) using the computer described below

28. 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.)*

29. Please tell us about the operating system (OS) on this computer:

    _____
    version # and name of OS (Windows might be Home, Pro, Education, Enterprise; Mac might be Catalina, Big Sur, Monterey)

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 *****"

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

Street Address	Building	Room #

VII. Workstation Security Protocols (completed by SysAdmin; submitted for each computer to be used)

☐ These are the protocols for the researchers named below who will use an institution-owned-and-maintained computer.

_____ _____ _____ _____ _____
researcher name *researcher name* *researcher name* *researcher name* *researcher name*

☐ These are the protocols this researcher _____ who is using a personally owned computer.
researcher name

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)	
Operating System is still being patched by vendor *(e.g., Windows 7 is no longer supported)* *Specify the OS:* _____	
Applications are still being patched by vendor that developed application. (*Examples are SAS and Stata)*	
Screen Saver is set to activate after 10 minutes of inactivity ***and screen is locked whenever researcher leaves the computer***. If controlled by GPO at campus-level, and more than 10 minutes, specify screen saver activation time: _____ If screensaver is activated on server, mark this "N/A."	

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