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 an External Hard Drive

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 must be obtained and sent to Add Health.

   _____ I agree to this condition.
   PI initials

6. Each user accessing the Add Health data must submit section IV of this form for review; access will not be granted until the form has 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, including user-created interim data analysis files or subsets of the data, may not be copied to any other media (including, but not limited to, CDs, flash drives, or the hard drive of the computer). 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. <u>External Hard Drive where the Add Health data will be stored and analyzed</u> (by PI and SysAdmin)

10. Please describe the external hard drive that will be used:

    <u>Note</u>: The external hard drive must:
    – have an external power source (it must be plugged into a power socket/outlet);
    – be considered a ***<u>desktop</u>*** model (not portable); and
    – be at least 1.5-2” deep, 5” high, and 6.5” wide.

    _____ _____
    make & model *vendor’s specifications for power type and dimensions or note that you are sending pictures of the EHD*

11. Who has physical access to the external hard drive?

12. Who has permission to use the external hard drive?

13. What is the secure storage location of the external hard drive?

Street Address	
Building	
Room #	
Storage Unit	

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

14. The external hard drive is not used by other projects.

    _____ I confirm that the EHD is not used by other projects.
    PI initials

15. The external hard drive will be connected only to a computer that is located in a private lockable office.

    _____ I agree to this condition.
    PI initials

16. Whole disk encryption has been enabled on the external hard drive storing the Add Health data with this software:

    _____ (e.g., Bitlocker, FileVault, Veracrypt)

17. I created separate directories on the external hard drive: one for the Add Health data and another for the program code and documentation to facilitate ease of backing up the program code and documentation.

    ◯ Yes ◯ No

18. Free space on the EHD must be cleared periodically and at the end of the contract period.

    ◯ The EHD is an SSD; I installed and will use this secure erasure software:
    Periodic erasure not required for SSD End-of-project software: _____

    ◯ The EHD is a spindle-type; I installed and will use this secure erasure software:
    Periodic erasure software: _____ End-of-project software: _____

III. Workstation Description ****** Submit this section for each computer that will be used with the EHD ******

Users (Researchers): _____ _____ _____ _____ _____

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

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

20. 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 *****"

21. Free space on the hard drive of the computer must be cleared periodically and at the end of the contract period.

    ☐ The computer's hard drive is an SSD; I installed and will use this secure erasure software:
    Periodic erasure not required for SSD End-of-project software: _____

    ☐ The computer's hard drive is a spindle-type; I installed and will use this secure erasure software:
    Periodic erasure software: _____ End-of-project software: _____

22. What is the physical location where this computer will be used when connected to the EHD that stores the Add Health data?

    Street Address

    Type of Building
    (e.g., private home, apartment complex, business office, campus office, etc.)

    Office or Room Description
    (e.g., private locked room, home office, keyed entry, card swipe entry, roommate, officemate, etc.)

23. Who has physical access to the computer?

24. Who has permission to use the computer?

25. Is the computer used by other projects?

    ☐ Yes ☐ No

26. Whole disk encryption has been enabled on the hard drive of this computer with this software:

    _____ (e.g., Bitlocker, FileVault, Veracrypt)

27. Access to the Add Health data must be restricted to project personnel using the security features available via the operating system (e.g., login to computer via userid/password and NTFS permissions to the external hard drive in Windows, ACLs in Linux and Macintosh Systems).

    _____ This has been implemented on the EHD for users currently using this computer.
    SysAdmin initials

    _____ I will implement this for all new users using this computer.
    SysAdmin initials

IV. User Set-Up and Agreements (by each user, initialed by SysAdmin)

28. My statistical applications have been configured to point the temporary working files to a temp directory on the encrypted external hard drive.

    Specify the drive and pathname of the temp directory: _____

29. Add Health requires passwords of at least 16 characters (passphrase: think "Longer is stronger").

    _____ I agree to this condition.
    user initials

30. Add Health requires that the screen saver:
    – activates after 7 minutes of inactivity; and
    – requires a password to log back in.

    _____ I have implemented this protocol.
    user initials

31. Add Health data must be excluded from the backup routine.

    _____ I agree to this condition.
    user initials

32. Add Health encourages researchers to back up their program code and documentation to a secondary source that may be removed from the office (e.g., a flash drive).

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

33. Where will hard copy information be printed?

34. 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

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

36. I will never connect the external hard drive to the computer while the network cable is plugged into the computer or while WiFi is enabled.

    _____ I agree to this condition.
    user initials

37. I will place the external hard drive on which the Add Health data resides in the locked cabinet, drawer, or safe specified above in #13 (see PI for location) when not in use.

    _____ I agree to this condition.
    user initials

38. I will not move the external hard drive to any other location than the working location specified above in #23 and the storage location specified above in #13 (see PI for location) (e.g., will not move it between office and home).

    _____ I agree to this condition.
    user initials

39. I will not leave my computer and external hard drive unattended while the external hard drive is attached.

    _____ I agree to this condition.
    user initials

40. I will not copy or move the Add Health data out of the secured directory on the external hard drive for any reason or by any means.

    _____ I agree to this condition.
    user initials

V. System Administrator

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

_____ I acknowledge that I consulted with the user (researcher).
System Administrator initials

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