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 (to be completed 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 for approval 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.

5. 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 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 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.

   Deletion of the interim data files will be done by ____ PI ____ ____________________________
   this designated research team member

   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.

_______ Add Health data will not be backed up by PI, IT, Researchers, or any other person.
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 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** on the EHD as approved in this Security Plan.

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

_______ I will not move any version of Add Health data from the secured directories on the EHD.
PI initials

_______ I will not copy any version of Add Health data for any reason or by any means.
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. External Hard Drive where the Add Health data will be stored and analyzed

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

Note: The external hard drive must:
– have an external power source (it must be plugged into a power socket/outlet);
– be considered a *desktop* 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?

Data Stored on an External Hard Drive

*(Page **3** of **8**)*

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 can be connected only to a computer that is located in a private lockable office.

_______ I will connect the EHD only to a computer that is located in a private lockable office.
PI initials

16. Whole Disk Encryption (WDE) is required for the external hard drive housing the Add Health data.

___________ I have activated WDE for this EHD.
SysAdmin initials

____
Name of WDE encryption software (e.g., Bitlocker, Veracrypt, FileVault)

17. The Add Health data (original provided by Add Health as well as variables created by researchers' code) must be kept in their own directories **separate from** researchers' program code and documentation to facilitate ease of backing up the program code and documentation without backing up the data.

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

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

______ Original Add Health data will reside in its own dedicated read-only directory on the approved EHD.
PI initials

______ Subsets of data created by code will reside in separate secured directories on the EHD.
PI initials

18. Statistical applications must be configured to point the temporary working files to the secured data directory on the EHD.

____
Pathname of secured directory where statistical applications point the temporary working file
*(The pathname should indicate the drive letter of the **EHD**, not the computer.)*

19. Free space on the external hard drive must be cleared periodically (spindle-type only).

□ The external hard drive is an SSD. Periodic erasure is not required for SSD.

□ The external hard drive is a spindle-type.
This secure erasure software has been installed and will be used: ________________

20. The Add Health data must be securely removed from the external hard drive at the end of the contract period.

□ The external hard drive is an SSD.
End-of-project protocol option #1: physically destroy the hard drive
End-of-project protocol option #2: encrypt, then reformat, then encrypt again
At end-of-project, I will use this protocol: ____

□ The external hard drive is a spindle-type.
End-of-project protocol option #1: physically destroy the hard drive
End-of-project protocol option #2: We will use this installed software: __________________________
At end-of-project, I will use this protocol: ____

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

Who uses this computer? ____________ ____________ ____________ ____________ ____________

researcher name *researcher name* *researcher name* *researcher name* *researcher name*

21. Please tell us about the computer being used to access the Add Health data that is stored on the EHD:

____________________ ________________________________ __ laptop __ desktop

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

22. 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, etc.)

To find the Windows 10 "name"

Press the Windows key (⊞)+R, type "dxdiag" in the pop-up window, see "Operating System"

To find the Mac OS "name"

From the Apple menu (), choose About This Mac, see "macOS *****"

23. Free space on the computer must be cleared periodically (spindle-type only) and at end-of-project.

□ The computer's drive is an SSD. Periodic erasure is not required for SSD.

□ The computer's drive is a spindle-type.
This secure erasure software has been installed and will be used: ________________

24. 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.)

25. Who has physical access to the computer?

Data Stored on an External Hard Drive
*(Page **6** of **8**)*

26. Who has permission to use the computer?

27. Is the computer used by other projects?

□ Yes □ No

28. Whole Disk Encryption (WDE) is required for the hard drive of computer accessing the Add Health data on the External Hard Drive.

___________ I have installed and activated WDE for this computer.
SysAdmin initials

____
Name of WDE encryption software (e.g., Bitlocker, Veracrypt, FileVault)

29. 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

System Administrator

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

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

IV. Agreements by Researcher: ______________________________ (PI and each Researcher submits individually)
Name of user signing this copy of this section

30. Strong passwords/passphrases are required.
    Add Health recommends:
    * Length of 16-30 characters is recommended ("longer is stronger")
    * Change a password/passphrase shorter than 16 characters *every 90 days*.
    * Change a password/passphrase of at least 16 characters *annually*.

    _________ Strong passwords as described above are required.
    user initials

31. The screen saver must be set to activate after no more than 10 minutes of inactivity and a password must be required to log back in.

    _________ Screen saver is set to activate after ______ minutes
    user initials

    _________ Password is required to log back in
    user initials

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

    _______ Add Health data is excluded from my backup routine.
    user initials

33. 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 can and should be backed up.
    user initials

    _______ I understand that this *does not include* permission to back up the data.
    user initials

    Describe your backup procedure:

34. Where will hard copy information be printed?

35. 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

36. If you will print hard copy information, describe how it will be handled/stored/discarded if differently from Q35.

37. It is required that you lock your screen before leaving your desk, and not rely on the screen saver timeout.

    On Windows computers: Press the Windows Key + the L Key: ⊞ Win + L

    On Mac computers: Press the Control Key + the Command Key + the Q Key: ^ + ⌘ + Q

    _______ I will always “Lock Before I Walk” rather than rely on the screen saver timeout.
    user initials

38. The external hard drive must never be connected to the computer while the network cable is plugged into the computer or while WiFi is enabled.

    ________ I will never connect the EHD to the computer while the network cable is plugged into the computer or while WiFi is enabled.
    user initials

39. The external hard drive on which the Add Health data must reside in the locked cabinet, drawer, or safe specified above in #13 (or see PI for location) when not in use.

    ________ I will place the EHD 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.
    user initials

40. The external hard drive must not be moved 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 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).
    user initials

41. The computer and external hard drive must never be left unattended while the external hard drive is attached.

    ________ I will not leave my computer and external hard drive unattended while the EHD is attached.
    user initials

42. The Add Health data must never be copied or moved out of the approved secured directory(ies) on the external hard drive for any reason or by any means.

    ________ I will not copy or move the original Add Health data out of the read-only secured directory on the EHD for any reason or by any means.
    user initials

    ________ I will not copy or move data I have created by programming code out of the the secured directory on the EHD for any reason or by any means.
    user initials