**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 Stand-Alone Computer*

All requests for data must include the following information.

**I.** **General Information (to be completed together 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.
    *PI initials*

5. Each user accessing the Add Health data must submit Section IV of this form (User Agreements) 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 stand-alone computer. ("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** 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 stand-alone computer.

   _____ I will not move any version of Add Health data from the secured directories on the computer.
   *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.  Detailed description of computer system where data will be stored and analyzed

10. Please tell us about the computer you are using to store the Add Health data:

   _____          _____          _____
   *brand/make*                    *model*                                 *confirm this is a desktop*
   *(e.g., Dell, Mac, etc.)*       *(e.g., Optiplex, Dimension, iMac Pro, etc.)*

11. Please tell us about the operating system (OS) on this computer:
    ("build" might be Home, Pro, Education, Enterprise, Catalina, Big Sur, Monterrey, and so on.)

   _____          _____          _____
   *name*                          *version*                               *build*

   | To find the Windows 10 "name" and "build" | 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 *****" |

12. What is the physical location of the computer?

   | | |
   |---|---|
   | Street Address | |
   | Building & Room # | |

13. The network interface card (NIC) must be removed or disabled so it cannot be used.

_____ Removed          _____ Disabled
*SysAdmin initials*                        *SysAdmin initials*

14. The Add Health data (original provided by Add Heath as well as variables created by researchers' code) must be kept in their own directories **separate from** researchers' program code and documentation **and separate from** non-Add Heath data 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** 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 stand-alone computer.

    _____ Original Add Health data will reside in its own dedicated read-only directory.
    *PI initials*

    _____ Subsets of data created by programming code will reside in a separate secured directory.
    *PI initials*

15. Whole Disk Encryption (WDE) is required for the hard drive of computer housing the Add Health data.

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

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

16. Printing

    _____ I confirm that a printer is attached to the computer.          _____ No printing will be done.
    *PI initials*                                                                                    *PI initials*

17. Free space on the computer must be cleared periodically (spindle-type only).

    ☐   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: _____

18. The Add Health data must be securely removed from the computer's hard drive at the end of the contract period.

    ☐   The computer's 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, then reformat again

    **At end-of-project, I will use this protocol**: _____

    ☐   The computer's 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.** **Security System to prevent unauthorized access to the data**

19. The computer must be configured to boot from the hard drive only and these new settings must be password-protected in the BIOS of the computer.

_____ Computer is configured to boot from the hard drive only.
*SysAdmin initials*

_____ These settings are password-protected.
*SysAdmin initials*

20. Access to the Add Health data is restricted to project personnel approved by Add Health using the security features available via the operating system (e.g., login via userid/password and NTFS permissions in Windows, ACLs in Linux and Macintosh Systems).

_____ Access is restricted as described above.
*SysAdmin initials*

21. 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.
*SysAdmin initials*

22. 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
*SysAdmin initials*

_____ Password is required to log back in
*SysAdmin initials*

23. The computer must be in a private, locked room, or the CPU must be physically locked down by either a cable attaching it to the desk or by a locking cabinet specifically designed for this purpose.

☐ Yes ☐ No The computer is kept in a private, locked room.

☐ Yes ☐ No The CPU is locked down by a cable.

☐ Yes ☐ No The CPU is in a locking cabinet.

24. Who has physical access to the stand-alone computer?

<br><br><br>

25. Who has permission to use the stand-alone computer?

<br><br><br>

26. Is the stand-alone computer used by other projects?

<br><br><br>

27. Will this computer be used to send and receive emails?

☐   Yes   ☐   No

28. Is this computer used to connect to the internet?

☐   Yes   ☐   No

---

## 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*

29. 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:

    |  |
    |---|

30. Where will hard copy information be printed?

    |  |
    |---|

31. 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*

32. If you will print hard copy information, describe how it will be handled/stored/discarded if differently from Q31.

    |  |
    |---|

33. 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*

34. 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 that you create with programming code must be stored in a separate secured directory on this same approved stand-alone computer.

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

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