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

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.

1b. **PI Institution** _____

PI contact information: Email: _____

Phone number: _____

System Administrator contact information: Email: _____
(your IT professional)

Name & Phone _____

2. Each project participant 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 the Carolina Population Center. A security pledge form can be found under Attachment D. Please copy for each participant.

   Number of security pledges included: _____

3. Only one complete copy of the Add Health data is permitted; however, time-delimited temporary data analysis files may be created. Temporary data analysis file(s) must be deleted every six months and recreated, as necessary, to complete analysis. Temporary data analysis files should be deleted upon completion of a project.

   All temporary data analysis files will be deleted _____ and _____ every year.
   month month

4. Add Health data, including temporary data analysis files or subsets of the data, may not be copied to other media such as CDs or diskettes to be used on other machines and platforms. 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.
   Investigator initial

II. Detailed description of computer system where data will be stored and analyzed

1. What type of **hardware and operating** system will be used?

Hardware *(Make/ Model*)

Operating System & Version:

2. What is the **physical location** of the hardware?

Street Address

Building

Room #

3. How are backups handled, and how will Add Health data be excluded from the backup routine? *SELECT ALL THAT APPLY*

☐ By checking this box, I agree that Add Health data will not be backed up.

☐ By checking this box, I understand that I may and should back up my program code and documentation, as described below.

4. Who has physical access to the equipment?

5. Who has permission to use the equipment?

6. Is the equipment used by other projects?

7. Where will hard copy info be printed?

8. How will hard copy data be handled/stored/discarded? *continued on next page*

Please check all three boxes to indicate you agree to these protocols.

☐ All printed copies of data output will be contained in a labeled folder.

☐ When not in use, paper copies will be stored in a locked filing cabinet.

☐ When researchers are no longer using the printouts, they will be shredded.

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

Street Address

Building

Room #

Storage Unit

III. Security system to prevent unauthorized access to the data

The following are minimum steps that should be taken to secure your **stand-alone** computer that houses the Add Health data. Please indicate below each security step you have implemented. Please write a short explanation if you cannot implement a specific step.

Physical Security of a Stand-Alone Computer

1. I configured the BIOS to boot the computer from the hard drive only. I will not allow the stand-alone computer to be booted from the diskette or CD-ROM drive.

☐ Implemented ☐ Not Implemented (please explain why not)

2. I password protected the BIOS so changes cannot be made to the BIOS without authorization.

☐ Implemented ☐ Not Implemented (please explain why not)

3. I secured the computer on which the Add Health data resides in a locked room, or secured the computer to a table with a lock and cable (locking the case so the battery cannot be removed).

☐ Locked room ☐ Lock and Cable ☐ Both a locked room and lock and cable

4. I removed or disabled the network interface card (NIC) so it cannot be used.

☐ Implemented ☐ Not Implemented (please explain why not)

Controlling Access to the Data

1. I restricted access to the Add Health data to project personnel 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).

☐ Implemented ☐ Not Implemented (please explain why not)

2. I require strong passwords.

☐ Implemented ☐ Not Implemented (please explain why not)

3. I activated a screen saver with password after 7 minutes of inactivity.

☐ Implemented ☐ Not Implemented (please explain why not)

4. I enabled **whole disk encryption for the hard drive of this computer.**

☐ Implemented ☐ Not Implemented (please explain why not)

Name of encryption software:

5. *N/A*

6. I installed and periodically run a secure erasure program. This program will be run **monthly** and after the secure data has been removed from the computer at the **end of the contract** period. *continued on next page*

☐ Implemented ☐ Not Implemented (please explain why not)

Name of **monthly** secure erasure software: _____

Name of **end-of-contract** secure erasure software: _____

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

   ◯ Yes ◯ No

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

   ◯ Yes ◯ No

9. I will not copy or move the Add Health data out of the secured directory for any reason.

   _____ I agree to this condition.
   Investigator initial

_____
Investigator initial

_____
SysAdmin (IT professional) initial