

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 the UNC SRW Server
administered by UNC Research Computing

NOTES AND INSTRUCTIONS

Throughout the Security Plan form:

- “PI” is the same as “Contract Investigator.”

Q1: List of users

- Include on this list ONLY those who will directly access the data.
 - Researchers (see definitions below)
- Do not include anyone who will not directly access the data.
 - Collaborators
 - IT
 - Contract Administrator
 - Officemates
- **Definitions:** Roles on an Add Health contract do not necessarily correlate to roles on a research project or at your institution.
 - **A Researcher** on an Add Health contract is defined as someone who has direct access to the Add Health data.
 - **A Collaborator** on an Add Health contract is defined as someone who is working with the contract’s researcher(s) in a way that does not involve direct access to the Add Health data on the contract.
 - **A Contract Administrator** is someone designated by the PI to handle the administrative tasks (requests, document submission, etc.) but who does not have any other role on the contract.
 - **An IT** is someone with IT expertise who assists with the storage of and access to the Add Health data but has no other role on the contract.
 - **An Officemate** is someone who shares an office (campus) or a home with a Researcher but who has no role on the contract.

Q11: Server Security Protocols

IT Security Awareness for End Users [↵] (e.g., https://its.cloudapps.unc.edu/info_security_awareness_training/) [↵]	↵
---	---

- This is the only line in the Section VII table that requires your response.
- It is not required that your institution offer IT Security Awareness, but we do want to know whether or not it does.

Section IV User Agreements

- The PI fills out this section in this form (other researchers will complete it in a separate document).

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 the UNC SRW Server
administered by UNC Research Computing

All requests for data must include the following information.

I. General Information (to be completed by PI)

1. List below the name(s) and responsibilities of those who will have access to the data (the PI, other investigators, and the research staff (students, research assistants, and programmers)
- *** Do not include IT, Contract Administrator, Officemates (i.e., no one who does not access the data).
- *** Changes in personnel require that this information be updated by email to Add Health Contracts.

--

2. Contact information:

Required: PI

Phone number: _____

Name: _____

Email: _____

Optional: person assisting PI

Phone number: _____

Name: _____

Email: _____

Required: Designated User Support Person**

Phone number: _____

Name: _____

Email: _____

**** Designated User Support Person** – Person on the contract's research team, or an IT staff member, who can help install software and who is familiar with remoting into a VDI workstation (or who can be trained by Add Health). This person will serve as your first level for questions and troubleshooting to help reduce the load on the Add Health staff. Examples of the support to be provided by this person include installing the VDI client on the researchers' computer and logging in to the SRW for the first time.

3. 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 (Attachment D) must be submitted to Add Health for approval before access is allowed.

PI initials

I agree to this condition.

4. Each user accessing the Add Health data must submit section IV of this form. Access will not be granted until the forms have been approved by Add Health.

PI initials

I agree to this condition.

Data Stored on a Server – UNC SRW
(Page 2 of 6)

5. Only one complete copy of the Add Health data is permitted.
- Users may create interim data analysis files and store them on 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.

Deletion of the interim data files will be done by _____
SPECIFY PI or this designated research team member

All interim data analysis files will be deleted in these two months each year:

_____ and _____
month month

6. 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

7. Not applicable for new applications

Contracts revising Security Plan: Original data CDs previously provided will be physically destroyed and before/after pictures submitted to Add Health.

_____ I agree to this condition.
PI initials

II. Detailed description of server system where data will be stored and Server Protocols

8. We will be using the remote compute server described below:

Virtual Desktop Infrastructure (VDI)Version:VMWare Horizon View 7.10

9. What is the physical location of the server hardware?

Street Address: 211 Manning Dr., Chapel Hill, NC 27599

Building & Room # ITS Manning – Data Center

10. We use an Enterprise environment, and are backing up the Add Health data in the following ways:

X Enterprise-level Server backup/archive: *Server Replication*

X Enterprise-level Server backup/archive: *Snapshots*

Enterprise-level Server backup/archive: *Tape or disk backup (must be encrypted)*

X Enterprise-level Server backup/archive: *Other, Specify:*

- We do hourly, daily and weekly snapshots.
- We keep the last 6 hourly, the last 2 daily and the last 2 weekly snapshots.

Data Stored on a Server – UNC SRW
(Page 3 of 6)

11. Server Security Protocols

<i>Please tell us whether you are using the specified protocol...</i>	Y or N
Internet Filtering [<i>special router ACLs or campus firewall</i>]	Y
Campus Filtering [<i>vlan ACLs or firewall</i>]	Y
Host-Based Firewall	Y
Intrusion Prevention System (e.g., Tipping Point)	Y
Managed and Monitored Malware Protection: Name/Version: _____	Y
Detailed Auditing for Access (account access)	Y
Detailed Auditing for Access to all Sensitive Files (file access)	Y Transfers, not VMs
Local System Event Logs	N
Remote Copy of System Event Logs	N
24/7 Monitoring (ping monitoring to ensure availability)	Y via Zabbix
Authenticated Operating System Vulnerability Scans (e.g., QualysGuard)	Y Images, not active VMs
Password Policy Enforcement (User and Administrator)	Y
Multi-Factor Authentication	Y
Encryption (File/Folder or Partition for all SI)	N
Least Functionality (i.e., installing only needed services. e.g., not IIS or SQL)	Y
Least Privilege (refers to user accounts, service accounts, and processes)	Y
Secure Physical Access	Y
IT staff configuring and maintaining system	Y
IT Security Awareness for End Users (e.g., https://its.cloudapps.unc.edu/info_security_awareness_training/)	
Warning Banner for Services Requiring Authentication	Y
Risk Assessment	Y
Patch Management Please specify: SCCM	Y
Vendor-Supported Operating System is still new enough to be getting patched/updated by vendor (<i>Windows XP, for instance, is no longer supported</i>)	Y
Vendor-Supported Applications are still new enough to be getting patched/updated by vendor(s) (<i>Examples are SAS and Stata</i>)	Y

12. Additional security protocols are attached at the end of this document.

No – there are no additional security protocols attached.

Data Stored on a Server – UNC SRW
(Page 4 of 6)

13. Who has physical access to the server equipment?

ITS Data center operations personnel only

14. Who has permission to use the server equipment?

Researchers and IT administrators

15. Is the server equipment used by other projects?

Yes; the SRW provides an isolated virtual environment for each user
Data and server access is managed by IT administrators.

III. SysAdmin confirmations

UNC Research Computing I acknowledge that I completed these Server Security Protocols.
System Administrator initials

Data Stored on a Server – UNC SRW
(Page 5 of 6)

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

16. Add Health encourages you to back up 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 I may and should back up my program code and documentation.
user initials

My backup procedure is:

We will rely on the UNC snapshots and Server Replication.

17. *This question not required for the SRW.*

18. *This question not required for the SRW.*

19. *This question not required for the SRW.*

20. All temp files reside on VM until logout; then VM/temp files are deleted (*no user response required here*).

21. I will not copy or move the Add Health data from the secured directory on the server for any reason or by any means.

_____ I agree to this condition.
user initials

V. Key Protocols

22. We are using a remote compute server to store the Add Health data.
23. We are using multifactor authentication (MFA) to connect to the Remote Compute Server.
24. Researchers' files (documentation, code, output) can be provided by request.
- * requested files must be put in a subfolder in the Work folder.
 - ... * name the folder by researcher name followed by the date (e.g., LASTNAME_2023-06-19).
 - ... * email the request (naming the PI of the contract, the contract number, and the file to be provided) to addhealth_contracts@unc.edu
 - ... * Add Health will provide the requested file(s) as quickly as possible, usually within two business days, to the person who made the request.
25. Vetting of files requested by a researcher will be done by **Add Health**.