Security Plans for Restricted-Use Data

Below are different locations where you might choose to store the Add Health data**.** Please make your selection and then read the associated document "How to secure ..." to see the essential components of a good security plan for that analysis/storage location.

Submit the completed Attachment A: Form to Describe Sensitive Data Security Plan for your analysis/storage location.

If your analysis/storage location is not listed, or if you need assistance with the security plan, please email addhealth_contracts@unc.edu. It is recommended that you ask for a consult with our security administrator prior to spending a large amount of time working through your local institution's security office and IRB.

Data stored on an Encrypted Stand-Alone Desktop Computer

A stand-alone computer is one that is in no way connected to another computer or networked device such as a switch, hub, or router.
The security plan form and information on how to secure a stand-alone computer are available at
How to secure a stand-alone desktop computer

Data stored on an Encrypted External Hard Drive

The external hard drive is a modified version of the stand-alone computer, in effect keeping the Add Health data off the Internet or a local area network (LAN), while using your daily-use computer.
The security plan form and information on how to secure an external hard drive are available at
How to secure an external hard drive

Data stored on a Server

There are two types of Servers possible.

The **most secure option** is a Compute Server:

- Files are stored on the server.
- All processing of the data files is done on the server.
- Data files are not served to the user's computer over the network.

The **least secure option** is a File Server:

- Files reside on the server.
- Files are served to the user's computer over the network and analyzed on the local computer.

The security plan form and information on how to secure a server are available at
How to secure a server

How to Secure a Stand-Alone Desktop Computer

A stand-alone desktop computer is one that is in no way connected to another computer or networked device, such as a switch, hub, or router (with the possible exception of a printer), or to the Internet or a local area network (LAN). The stand-alone desktop computer can be running Windows 10 client or server, Linux, or Mac OS X. Because the stand-alone desktop computer is not connected to the Internet or a local or wide area network, the emphasis for securing the data is placed on physical security of the computer and controlling access to the data.

Here are the minimum steps you should take to secure the Add Health data on your stand-alone desktop computer:

Physical Security of a Stand-Alone Computer

1. Configure the BIOS to boot the desktop computer from the hard drive only. Do not allow the stand-alone desktop computer to be booted from the diskette or CD-ROM drive.
2. Password protect the BIOS so changes cannot be made to the BIOS without authorization.
3. Secure the desktop computer on which the Add Health data resides in a locked room, or secure the desktop computer to a table with a lock and cable (locking the case so the battery cannot be disconnected, which would disable the BIOS password).
4. Remove or disable the network interface card (NIC) so it cannot be used.
5. Store the data on a desktop computer only. Laptops may not be used to store the Add Health data.

Controlling Access to the Data

1. Restrict 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 10, ACLs in Linux and OS X).
2. Require strong passwords.
   - You can run L0phtcrack to look for bad passwords.
   - You can enable password complexity.
3. Password protect screen saver and activate after three minutes of inactivity.
4. Enable whole disk encryption (e.g., *Bitlocker, PGP Whole Disk Encryption, FileVault2, Veracrypt*) or directory-based encryption (e.g., *Windows Encrypting File System* or *Veracrypt*) for directories containing secure data.
5. Configure your analysis software to point temporary work files to the encrypted Add Health data directory.

6. Install and periodically run a secure erasure program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period. (*Heidi is free and works well*. SDELETE also works well and can be scripted.)
7. Do not copy or move the Add Health data out of the secured directory for any reason.

Back to Security Plans for Restricted-Use Data

How to Secure an External Hard Drive

For one to three users who are willing to schedule time accessing the data, a stand-alone computer attached to an encrypted external hard drive with an emphasis placed on physical security of the computer and controlling access to the data can be one of the most secure computing platforms for your sensitive data. An external hard drive is a modified version of the stand-alone computer, in effect keeping the Add Health data off the Internet or a LAN, even though you may be using your main computer that is normally connected to the internet.
The emphasis for securing the data on an external hard drive is placed on removing the computer from the network while the external hard drive is in use, controlling access to the data directory, and physically securing the hard drive in a locked cabinet when not in use.

USB "thumb/jump" drives are not acceptable devices for this option. USB external hard drives, Firewire external hard drives, or EIDE hard drives in a Startech-type of removable device are acceptable options. **The external hard drive must be larger than purse or pocket size**. These external hard drives are sometimes classified as *desktop models* and must be plugged into an electrical outlet when in use.
Use of a laptop with the external hard drive is permitted, however the laptop must be secured to a desk by lock and cable.

To make this scenario work, you need remember and do only two things:

1. Never have the network cable and external hard drive connected to the computer at the same time.
2. Always secure the external hard drive in a locked cabinet, drawer, or safe when not in use.

Prerequisites for placing the Add Health data on an external hard drive:

1. You need a private, lockable office, not a student computer lab.
2. You need your statistical analysis applications installed on your local hard drive, not on a network server.
3. You may need a new local userid on your PC, since you may not be able to use your Domain Account, unless you are able to login without an internet connection (e.g., credentials are cached).
4. You must use an operating system that is currently being patched and supported by the vendor (e.g., Windows 10, Mac OS X, or Linux). You may not use Windows 95, 98, NT4, or XP. If you are unsure whether or not your operating system is currently supported, do an internet search on your operating system with the word "lifecycle." This should give you the vendor's timeline for supporting the operating system. For example, searching "Windows Lifecycle" shows the Microsoft page detailing the years during which their operating systems will be supported.
5. You must not move the external hard drive from the location specified in your security plan (e.g., cannot move between office and home).

Follow these steps to prepare your computer for use with the Add Health data on an external hard drive:

1. Power down the computer, which resides in a locked room accessible by authorized personnel only.
2. Disconnect the network cable.
3. Connect the external hard drive.
4. Power up the computer.
5. Login using the local userid created for accessing the Add Health data.
6. Create separate directories on the external hard drive for the Add Health data and your program files.
7. Encrypt the entire external hard drive with either Bitlocker, PGP Whole Disk Encryption, Veracrypt or another whole disk encryption program, or encrypt the sensitive data directory on the external hard drive using Windows' Encrypting File System or Veracrypt or similar encryption program. (Make sure you do not encrypt your program and documentation directories unless you are using Whole Disk Encryption.)
8. Configure your analysis software to point temporary work files to the encrypted Add Health data directory on the external hard drive.
9. Password protect your screen saver and activate after three minutes of inactivity.
10. Install and periodically run a secure erasure program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period. (*Heidi is free and works well*. SDELETE also works well and can be scripted.)

Follow these steps each time you use the Add Health data external hard drive:

1. Power down the computer.
2. Disconnect the network cable. (Creating a hardware profile that disables the network interface card is an acceptable substitute for disconnecting the network cable.)
3. Connect the external hard drive.
4. Power up the computer.
5. Login using your local userid.
6. Do not leave your computer and external hard drive unattended.
7. Do not copy or move the Add Health data out of the secured directory on the external hard drive for any reason.

Follow these steps when you are not using the Add Health data external hard drive:

1. Logout.
2. Power down the computer.
3. Disconnect the external hard drive.
4. Lock the external hard drive in a secure place (e.g., a file cabinet, drawer, or safe).
5. Connect the network cable.

Back to Security Plans for Restricted-Use Data

How to Secure a Server

A server can be configured as a File Server or a Compute Server. There are advantages and disadvantages of each.

File Server

Windows File Server, Linux SAMBA server, or Storage Area Network (SAN) CIFS Share: A file server "serves" files across the wire to the client machine requesting access. This does not require high-end hardware to serve files to many clients. However, the files end up on the user's computer, which we want to avoid when dealing with sensitive data. The emphasis for securing the data on a file server is placed on securing the server, redirecting all files (including temporary statistical analysis files) back to the server share, and securing the user's local computer.

Compute Server *(Preferred)*

Windows Terminal Server and Linux Compute Server: A compute server stores and processes all files directly on the server: files do not cross the wire to the user's computer. The security benefit to using a compute server is that all of the sensitive files stay on the server. However, the compute server environment typically requires higher-end servers with more processing power and memory to accommodate a large number of users. While we still need to evaluate the security posture of the user's computer, the main emphasis for securing data on a compute server is securing the compute server and the communication tunnel between the server and the user's computer.

The security plan form contains two tables of security controls: one for the server and one for the user's local computer. The link below offers an explanation of the security controls for both the server and workstation:

- Explanation of Security Controls Standards referenced in "Form to describe your security plan"

Back to Security Plans for Restricted-Use Data

Choose a Good Password

A good password SHOULD

- be at least 16 characters in length
- be a multiple of seven characters (7, 14, or 21) (for Windows)
- use at least one non-alphanumeric character. These are: ~!@#$%^&*()_+-={}|[]\:";'<>?,./`
- use at least one numeric character (0-9)
- use a mix of upper and lower case letters
- be very different from the last password used for that account (at least four characters not used in the previous one)
- be changed often (i.e., at least every 90 days)

A good password SHOULD NOT

- include any personal information about you (e.g., nicknames, initials, login name, SSN#, address, birthday)
- include any personal information about your relatives
- include any information about your work (e.g., office number, project name)
- be the name of any computer (e.g., dell, unix)
- be written down anywhere or in any file on any of your accounts
- see www.xkcd.com/936

Back to Security Plans for Restricted-Use Data

Redirect Temporary Work Files

Statistical applications may create temporary data sets during the execution of your programs. The location of these temporary working directories can be specified for each statistical application. You should configure your statistical analysis software to point the temporary work files to an encrypted temporary data directory (i.e., e:\tmpDATA) to ensure portions of your data set are not accessible by unauthorized individuals. You should then run the secure erasure program on this temporary data directory periodically.

Following are some popular statistical applications and directions for redirecting the temporary working directories.

MPlus

- To set Mplus to use a secured directory for temporary files, create the FORT_TMPDIR environment variable and assign it the name of the secured directory.

R

- Environment variables can be set for Rgui.exe and Rterm.exe in three different ways. See the following URL for instructions.
- https://cran.r-project.org/bin/windows/base/rw-FAQ.html#How-do-I-set-environment-variables_003f

SAS

- Add the following to the end of the "Target/Command" line in the properties of the SAS shortcut: -work "drive_letter:\secure_directory" (i.e.: -work "e:\ahd\tmpSAS").

SPSS

- In SPSS you need to manually set the temporary working directory. This is done under *Edit*, *Options*, *Temporary Directory*.

Stata

- To point temporary Stata files to a secured directory, you need to set an environment variable called STATATMP and point it to the secured directory (i.e., e:\ahd\tmpSTATA).
- See http://www.stata.com/support/faqs/data/statatmp.html for more details.

Back to Security Plans for Restricted-Use Data

Links to Security Resources

The following web sites are listed here for your reference. Reading these pages is not mandatory for securing your computer for the Add Health data, but may provide more detailed information than the pages listed under "How to Secure…".

General Guides

- SANS/FBI Top 20 List
- SANS Security Step-by-Step Guides
- NSA security guides: Browse to https://www.nsa.gov/index.shtml and search for “security guides”
- Internet Connection Security for Windows Users by Gibson Research Corporation
- CERT
- SecurityFocus
- Common Vulnerabilities and Exposures
- The Center for Internet Security
- Microsoft Security

Unix Security

- General Linux Security
- Suse Linux
- Red Hat Security Guide

Windows Security

- Windows Server 2012
- Windows Server 2008 R2
- Windows 7
- Windows 8

Macintosh Security

- Apple Computer's Security Updates (Search for "Security Updates")
- Macintosh Security Site
- Apple Developer OSX Security
- MacWrite

Back to Security Plans for Restricted-Use Data