ENTERPRISE TECHNOLOGY SERVICES | University of California Santa Barbara

Secure Compute Research Environment (SCRE)

RESTRICTED DATA PROVIDER REQUIREMENTS CROSSWALK

Provider Name: UNC Carolina Population Center, Add Health

Date Requirements retrieved: March 10, 2015
Source Requirements retrieved from:
http://www.cpc.unc.edu/research/tools/datasecurity

Requirements – taken from "Windows Computer Connected to Network" and "Redirect Temporary Work Files" documents

#	Requirement	Met? (Yes/No)	Notes
1	Temporary data analysis files must be deleted every six months and recreated, as necessary, to complete analysis.	Yes	Eraser set to delete all files and subdirectories of Z:\USERTMP once a month
2	Temporary data analysis files should be deleted upon completion of a project.	Yes	VM images secure erased at end of project
3	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.	Yes	No copying of AddHealth data to
4	Require strong passwords	Yes	Windows login and BitLocker volume password requirement: 14-characters with at least one lowercase letter, one uppercase letter and one number required
5	Activate screen saver with password after three minutes of activity	Yes	Session timeout enabled
6	Install encryption software for directories containing secure data (e.g. Windows 7/8 encryption)	Yes	BitLocker
7	Configure statistical applications to point the temporary working files to the secured data directory	Yes	Configured environment variables and applications settings for Stata, SAS, SPSS to store temporary files in encrypted volume Z:
8	Install 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.	Yes	Eraser is run once a month on the USERTMP directory and will be run at the end of the contract period as well.
9	Do not copy or move the AddHealth data out of the secured directory for any reason	Yes	Researcher agreement
10	Do not install IIS or MS SQL server on the Windows computer that houses sensitive data	Yes	IIS and MS SQL server not installed
11	Turn off all unneeded services and disable	Yes	Unnecessary services and

	unneeded network protocols		protocols disabled according to VMWare Horizon View Optimization Guide for Win7
12	Disable Windows File and Printer Sharing	Yes	No file sharing enabled
13	Do not enable file sharing on local Windows machines	Yes	No file sharing enabled
14	Remove the Everyone group from the Access this Computer from the Network user right	Yes	Removed Everyone group from rights
15	Disable the Guest account	Yes	Guest account disabled
16	Replace the Everyone group with the appropriate group(s) on critical system folders, files and registry keys	Yes	Removed Everyone group from shares
17	Remove, disable or rename administrative shares	Yes	No admin shares
18	Restrict/prevent anonymous access and enumeration of accounts and shares	Yes	No anonymous access, accounts or shares
19	Create a new userid for administrative purposes and remove the original administrator userid's administrative privileges.	Yes	Separate operator credentials
20	Install and maintain all OS and application security patches	Yes	Check daily for patches and updates
21	Install an antivirus software program and keep the virus definition files updated	Yes	Microsoft Security Essentials installed, updates daily
22	Secure performance data	N/A	N/A for Windows 7 hosts
23	Enable auditing and check logs often	Yes	Syslog being sent to central syslog
24	Disable or remove Windows Scripting Host	Yes	disabled
25	Use a corporate, hardware or software firewall	Yes	Windows firewall installed and configured on research hosts and admin hosts, ACLs on private networks
26	Redirect Temporary Work Files	Yes	Configured environment variables for system to store temporary files in encrypted volume Z: