SECURITY BEST PRACTICES – Level 2b

Revised 4/11/2007

Introduction

The data sets provided in conjunction with this agreement are controlled access data. The procedures described below are based on the assumption that access to deidentified person level detailed genomic data associated with phenome data should be controlled and not publicly available.

The goal of this process is to ensure that data provided by the NIH is kept sufficiently secure and not released to any person not permitted to access the data, either through malicious or inadvertent means. To accommodate these requirements, systems housing these data must not be directly accessible from the internet, and the data must not be posted on any web or ftp server. Data placed on shared systems must be secured and limited to those involved in the research for which the data has been requested. If data is stored on laptops or removable devices, those devices must be encrypted.

Protecting the Security of Controlled Data

Security Awareness Requirements

The controlled access data you received is considered sensitive information. By following the **best practices** below, you will be doing much towards protecting the information entrusted to your care. This is a minimum set of requirements; additional restrictions may be needed by your institution and should be guided by the knowledge of the user community at your institution.

Think Electronic Security

1. ***The Single Most Important Advice:*** Download data to a secure computer or server and not to unsecured network drives or servers.

2. Make sure these files are never exposed to the Internet. Data must never be posted on a PI's (or institution's) website because the files can be "discovered" by internet search engines, e.g., *Google, MSN*.

3. Have a strong password for file access and never share it.

4. If you leave your office, close out of data files or lock your computer.

    * Install a password-enabled screen saver that activates after 15 minutes of inactivity.

6. Laptops that are hold the controlled access data must be encrypted. Most operating systems have the ability to natively run an encrypted file system (Windows = EFS or Pointsec and Mac OSX = File Vault.

Think Physical Security

1. If the data are in hard copy or reside on portable media, e.g., on a CD, flash drive or laptop), treat it as though it were cash.

2. Don't leave it unattended or in an unlocked room.

3. Consider locking it up.

4. Exercise caution when traveling with portable media, i.e., take extra precautions to avoid the possibility of loss or theft (especially flash drives which are small and can easily be misplaced).

Protecting the Security of Controlled Data on Servers

1. Servers must not be accessible directly from the internet, (i.e. must be behind a firewall or not connected to a larger network) and unnecessary services disabled.

2. Keep systems up to date with security patches

3. dbGaP data on the systems must be secured from other users (restrict directory permissions to only the owner and group) and if exported via file sharing, ensure limited access to remote systems.

4. If accessing system remotely, encrypted data access must be used (such as SSH). It is preferred to use a tool such as RDP, X-windows or VNC that does not permit copying of data and provides "View only" support.

5. Ensure that all users of this data have IT security training suitable for this data access and understand the restrictions and responsibilities involved in access to this data.

6. If data is used on multiple systems (such as a compute cluster), ensure that data access policies are retained throughout the processing of the data on all the other systems. If data is cached on local systems, directory protection must be kept, data must be removed when processing is complete.

Requesting Investigators must meet the spirit and intent of these protection requirements to ensure a secure environment 24 hours a day for the period of the agreement.

Use Data by Approved Users on Secure Systems

The requesting investigator must retain the original version of the data encrypted data. The requesting investigator must track any copies or extracts made of the data and shall make no

copy or extract of the subject data available to anyone except an authorized staff member for the purpose of the research for which the subject data were made available.

Collaborating investigators from other institutions must complete an independent data use certification to gain access to the data.

When use of the dataset is complete—destroy all individually identifiable data

1. Shred hard copies.

2. Delete electronic files securely:

3. At minimum, delete the files and then empty your recycle bin.

4. Optimally, use a secure method, e.g., an electronic "shredder" program that performs a permanent delete and overwrite.

Additional Resources for testing and best practices:

The Center for Internet Security

"CIS is the only distributor of consensus best practice standards for security configuration. The Benchmarks are widely accepted by U.S. government agencies for FISMA compliance, and by auditors for compliance with the ISO standard as well as GLB, SOx, HIPAA, FIRPA and other the regulatory requirements for information security. End user organizations that build their configuration policies based on the consensus benchmarks can not acquire them elsewhere."

http://www.cisecurity.org/.

Appendix A – Has checklists based on CIS best practices, customized for dbGaP data use.

Appendix A:

Best Practice Security Requirements for dbGaP Data Recipients

Preface

This appendix has been adapted from the HHS IT Security program for minimal security standards and the Center for Internet Security, and adapted as "Best Practices" for dbGaP

Introduction

The *dbGaP Best Practices Guidelines* Checklists were created to provide guidance and expectation on how to treat the controlled access data received from dbGaP.

Purpose

The purpose of this appendix is to provide minimum configuration standards for recipients of data from dbGaP. Adhering to these procedures will provide a baseline level of security, ensuring that minimum standards or greater are implemented to secure the confidentiality, integrity, and availability of data resources. If local IT policies are more restrictive, then local policies should apply.

Background

Minimum security configuration standards help to ensure sound control of each system. Adhering to minimum standards helps to mitigate risks associated with implementing applications and software by providing a solid foundation to track changes, the differences between versions, and new components as they are installed. System and application default settings are not optimal from a security perspective. Using default settings increases the risk of exploitation. These risks are mitigated through the use of minimum security configuration standards.

Windows 2003 Server

Windows 2003 Professional Configuration Guide					
Category	800-53	800-53 Map	Action	Completed	Comments
Access Controls	Access Enforcement	AC-3	Only allow Server Administrators to Schedule Tasks	"X", "*", or "N/A"	Required if "*" in previous column.
Access Controls	Access Enforcement	AC-3	Do Not Allow Automatic Administrative Logon		
Access Controls	Access Enforcement	AC-3	Configure all disk volumes to use the NTFS file system		
Access Controls	Access Enforcement	AC-3	Set Unsigned Driver Installation Behavior To "Warn but allow installation" or "Do not allow installation"		
Accounts	Account Management	AC-2	Rename and enable Administrator Account		
Accounts	Account Management	AC-2	Rename and disable the Guest Account		
Accounts	User Identification and Authentication	AC-3 AC-7 IA-2 IA-5	Configure the system per 800-53 Account Policy Control Requirements		
Accounts	Account Management	AC-2	Do not allow anonymous enumeration of SAM accounts		
Accounts	Account Management	AC-2	Do not allow anonymous enumeration of SAM accounts and shares		
Accounts	Account Management	AC-2	Disable anonymous SID/Name translation		
Accounts	Account Management	AC-2	Limit local account use of blank passwords to console logon only		
Device	Session Lock	AC-11	Disable allowing users undock without having to log on		
Logon	User Identification and Authentication	IA-2	Configure the system to display a warning banner.		
Logon	User Identification and Authentication	IA-2	Do Not Allow System to be Shut Down Without Having to Log On		
Logon	User Identification and Authentication	IA-2	Enable CTRL+ALT+Delete Requirement for Logon		
Media	Remote Access	AC-17	Restrict CD-ROM Access to Locally Logged-On User Only		
Media	Remote Access	AC-17	Restrict Floppy Access to Locally Logged-On User Only		
Network Access	Account Management	AC-2	Disable letting Everyone permissions apply to anonymous users		
Network Access	Remote Access	AC-17	Digitally Encrypt Secure Channel Data		
Network Access	Remote Access	AC-17	Digitally Sign Client Communication		

Windows 2003 Professional Configuration Guide

Category	800-53	800-53 Map	Action	Completed	Comments
Network Access	Remote Access	AC-17	Digitally Sign Server Communication		
Network Access	Remote Access	AC-17	Require Strong (Windows 2000 or later) Session Key		
Network Access	Remote Access	AC-17	Disable Sending Unencrypted Password to Connect to Third-Party SMB Servers		
Network Access	Remote Access	AC-17	Restrict anonymous access to Named Pipes and Shares		
Network Access	Remote Access	AC-17	Configure system so that no shares can be accessed anonymously		
Network Access	Transmission Integrity	SC-8	Do not allow storage of credentials or .NET passports for network authentication		
Network Security	Information Remnants	SC-4	Do not store LAN Manager password hash value on next password change		
Network Security	User Identification and Authentication	IA-2	Configure LAN Manager Authentication Level to "Send NTLMv2 response only\refuse LM"		
Password Management	Access Enforcement	AC-3	Do Not Store Passwords Using Reversible Encryption		
Password Management	Authenticator Management	IA-5	Disable System Maintenance of Computer Account Password (Domain Controllers)		
Patches	Flaw Remediation	SI-2	Apply critical Operating System security patches		
Patches	Flaw Remediation	SI-2	Ensure That Before the System is Loaded Onto an Operational Network, Security Patches, Service Packs, And Hot Fixes are all Tested		
Permissions	Access Enforcement	AC-3	Configure the system to provide least access to shared folders		
Service	Least Functionality	CM-7	Configure permissions for the following services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause.' Alerter (Alerter) Client Service for NetWare (NWCWorkstation) Clipbook (ClipSrv) Fax Service (Fax) File Replication (NtFrs) File Server for Macintosh (MacFile) FTP Publishing Service (MSFtpsvc) Help and Support (helpsvc) HTTP SSL (HTTPFilter) IIS Admin Service (IISADMIN) Indexing Service (cisvc) License Logging Service (LicenseService) Messenger (Messenger) Microsoft POP3 Service NetMeeting Remote Desktop Sharing (mnmsrvc) Network Connections		

Windows 2003 Professional Configuration Guide

Category	800-53	800-53 Map	Action	Completed	Comments
			Network News Transport Protocol (NNTP) (NntpSvc) Print Server for Macintosh (MacPrint) Print Spooler (Spooler) Remote Access Auto Connection Manager (RasAuto) Remote Access Connection Manager (RasMan) Remote Administration Service Remote Desktop Help Session Manager (RDSessMgr) Remote Installation (BINLSVC) Remote Procedure Call (RPC) Locator (RpcLocator) Remote Registry Service (RemoteRegistry) Remote Server Manager (AppMgr) Remote Server Monitor (Appmon) Remote Storage Notification (Remote_Storage_User_Link) Remote Storage Server (Remote_Storage_Server) Simple Mail Transfer Protocol (SMTP) (SMTPSVC) SNMP Service (SNMP) SNMP Trap Service (SNMPTRAP) Telephony (TapiSrv) Telnet (TlntSvr) Terminal Services (TermService) Trivial FTP Daemon (tftpd) Wireless Configuration (WZCSVC) World Wide Web Publishing Services (W3SVC)		
Service	Least Functionality	CM-7	Review all services for proper configuration and disable unneeded services		
Registry Permission	Least Functionality	CM-7	Remove administrative shares on servers		
User Rights	Access Enforcement	AC-3 AU-8 AU-9	Audit user rights assignments to ensure they are appropriately applied		

Windows XP Professional

Windows XP Configuration Guide					
Category	**800-53**	**800-53 Map**	**Action**	**Completed**	**Comments**
Access Controls	Access Enforcement	AC-3	Do Not Allow Automatic Administrative Logon	"X", "*", or "N/A"	Required if "*" in previous column.
Access Controls	Access Enforcement	AC-3	Configure all disk volumes to use the NTFS file system		
Access Controls	Access Enforcement	AC-3	Enable account lockout after specific length of time		
Access Controls	Access Enforcement	AC-3	Set Unsigned Driver Installation Behavior To "Warn but allow installation" or "Do not allow installation"		
Accounts	Account Management	AC-2	Rename Administrator Account		
Accounts	Account Management	AC-2	Rename and disable the Guest Account		
Accounts	User Identification and Authentication	AC-3 AC-7 IA-2 IA-5	All passwords should be strong passwords, and account names longer than 6 characters		
Logon	User Identification and Authentication	IA-2	Configure the system to display a warning banner.		
Logon	User Identification and Authentication	IA-2	Do Not Allow System to be Shut Down Without Having to Log On		
Logon	User Identification and Authentication	IA-2	Enable CTRL+ALT+Delete Requirement for Logon		
Media	Remote Access	AC-17	Restrict CD-ROM Access to Locally Logged-On User Only		
Media	Remote Access	AC-17	Restrict Floppy Access to Locally Logged-On User Only		
Network Access	Remote Access	AC-17	Digitally Encrypt Secure Channel Data		
Network Access	Remote Access	AC-17	Digitally Sign Server Communication		
Network Access	Remote Access	AC-17	Disable Sending Unencrypted Password to Connect to Third-Party SMB Servers		
Password Management	Authenticator Management	IA-5	Do Not Display Last User Name		
Password Management	Authenticator Management	IA-5	Mask password text fields		

Windows XP Configuration Guide

Category	800-53	800-53 Map	Action	Completed	Comments
Password Management	Authenticator Management	IA-5	Domain Members: Disable Machine Account Password Changes		

Patches	Flaw Remediation	SI-2	Service Packs and Security Updates
			  Test all software and patch updates
			  Install all Major Service Packs and Security Updates
			  Install all critical security updates as issued by the software developer		

Registry Permission	Least Functionality	CM-7	Disable automatic execution of CD applications		
Registry Permission	Least Functionality	CM-7	Disable CD Autorun		
Registry Permission	User Identification and Authentication	IA-2	Disable Automatic Logon		
Service	Least Functionality	CM-7	Configure permissions for the following services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause.' Alerter Clipbook Computer Browser Fax Service FTP Publishing Service IIS Admin Service Indexing Service Messenger Net Logon NetMeeting Remote Desktop Sharing Network DDE Share Database Manager Network Dynamic Data Exchange (DDE) Remote Desktop Help Session Manager Remote Registry Service Routing and Remote Access Simple Mail Transfer Protocol (SMTP) Simple Network Management Protocol (SNMP) Service Simple Network Management Protocol (SNMP) Trap SSDP Discovery Service Task Scheduler		

Windows XP Configuration Guide

Category	800-53	800-53 Map	Action	Completed	Comments
			Telnet Terminal Services Universal Plug and Play Device Host World Wide Web Publishing Services		
Service	Least Functionality	CM-7	Disable all services that do not directly support the role of the workstation		

Linux Variants

Linux Variants Configuration Guide

Category	800-53	800-53 Map	Action	Completed	Comments
Accounts / Access	Account Management	AC-2	No '.' (current working directory) or group/world writable files exist in root's $PATH.	"X", "*", or "N/A"	Required if "*" in previous column.
Accounts / Access	Account Management	AC-2	Install TCP Wrappers		
Accounts / Access	Account Management	AC-2	Remove user .netrc files		
Accounts / Access	Account Management	AC-2	Set "mesg n" as default for all users		
Accounts / Access	Account Management	AC-2	Set default group for root account		
Accounts / Access	Account Management	AC-2	Verify that no UID 0 accounts exist other than root		
Accounts / Access	Access Enforcement	AC-3	Set project directories to be as restrictive as possible to the research group		
Accounts / Access	Access Enforcement	AC-3	Set Account Expiration Parameters On Active Accounts		
Accounts / Access	Access Enforcement	AC-3	Require Authentication For Single-User Mode		
Accounts / Access	Access Enforcement	AC-3	Remove rhosts support in pam		
Accounts / Access	Access Enforcement	AC-3	Remove empty crontab files and restrict file permissions to authorized users		
Accounts / Access	Access Enforcement	AC-3	Restrict at/cron to authorized users		
Accounts / Access	Access Enforcement	AC-3	Restrict root logins to system console or ssh on local network		
Accounts / Access	Access Enforcement	AC-3	Set LILO/GRUB Password if possible, or set password before boot		
Accounts / Access	System Use Notification	AC-8	Set a warning banner for console and GUI based logins.		
Auditing	Auditable Events	AU-2	Enable system accounting (Install the sysstat package if needed).		
Installation / Patches	Transmission Integrity	SC-8	Utilize Secure Shell (SSH) for remote logins and file transfers.		
Patches,	Flaw Remediation	SI-2	Apply critical Operating System security patches		
Misc / Tuning	Information Flow Enforcement	AC-4	Deny all network access to the system via hosts.deny; Explicitly allow network connections, either all services selected ones, from the local		

Linux Variants Configuration Guide

Category	800-53	800-53 Map	Action	Completed	Comments
			network and selected hosts via hosts.allow		
Misc / Tuning	Information Flow Enforcement	AC-4	Add ' nosuid' and ' nodev' Option For Removable Media In /etc/fstab		
Auditing	Protection of Audit Information	AU-9	Unless the host is functioning as a syslog server, prevent the system from accepting syslog messages from the network.		
Misc / Tuning	Least Functionality	CM-7	Set default UMASK for users, directories, and files to meet the needs of the system		
Misc / Tuning	Least Functionality	CM-7	Disable Core Dumps		
Services	Least Functionality	CM-7	Disable xinetd if none of its services are used		
Services	Least Functionality	CM-7	Disable Sendmail and other inbound mail daemons		
Services	Least Functionality	CM-7	Disable GUI Logon		
Services	Least Functionality	CM-7	Disable X-Windows		
Services	Least Functionality	CM-7	Disable standard boot services that do not support the role of the system		
Services	Least Functionality	CM-7	Turn off standard services except those needed for the system's role.		
Logon	User Identification and Authentication	IA-2	Configure the system to display a warning banner.		
Accounts / Access	Authenticator Management	IA-5	No "+" entries should exist in /etc/passwd or /etc/group.		

MacOS X – Desktop

These recommendations are under development, the following set of recommendations is an initial set of rules to use for configuring an OS X desktop.

Mac OS X					
Category	**800-53**	**800-53 Map**	**Action**	**Completed**	**Comments**
Accounts / Access	Account Management	AC-2	No '.' (current working directory) or group/world writable files exist in root's $PATH.	"X", "*", or "N/A"	Required if "*" in previous column.
Accounts / Access	Account Management	AC-2	Normal use login as user not as an administrator		
Accounts / Access	Access Enforcement	AC-3	Set project directories to be as restrictive as possible to the research group		
Accounts / Access	Access Enforcement	AC-3	Remove empty crontab files and restrict file permissions to authorized users		
Accounts / Access	Access Enforcement	AC-3	Restrict at/cron to authorized users		
Accounts / Access	Access Enforcement	AC-3	Restrict root logins to system console or ssh on local network		
Accounts / Access	System Use Notification	AC-8	Set a warning banner for console and GUI based logins.		
Auditing	Auditable Events	AU-2	Enable logging		
Installation / Patches	Transmission Integrity	SC-8	Utilize Secure Shell (SSH) for remote logins and file transfers.		
Patches,	Flaw Remediation	SI-2	Apply critical Operating System security patches		
Misc/Tuning	Least Functionality	CM-7	Disable Bluetooth		
Misc / Tuning	Least Functionality	CM-7	Disable Core Dumps		
Services	Least Functionality	CM-7	Turn off standard services except those needed for the system's role.		
Logon	User Identification and Authentication	IA-2	Configure the system to display a warning banner.		
Accounts / Access	Authenticator Management	IA-5	No "+" entries should exist in /etc/passwd or /etc/group.		

For Mac Laptops, an encryption tool such as FileVault should be used to protect all controlled access data.

DRAFT