PDBP
Parkinson's Disease
Biomarkers Program

DMR Best Practices Requirements

Security Best Practices

PDBP
Parkinson's Disease
Biomarkers Program

Table of Contents

1. 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 de-identified 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 DMR 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.

2. Protecting the Security of Controlled Data

2.1. 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.

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

6. Data stored on laptops must be encrypted. Most operating systems have the ability to natively run an encrypted file system or encrypt portions of the file system. (Windows = EFS or Pointsec and Mac OSX = File Vault).

2.1. 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).

3. 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. DMR 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 or VPN). 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, and 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.

4. 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 data 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, FERPA and other 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/.