Recommended Practices for Safeguarding Access to Confidential Data

To provide a secure working environment for use and storage of source data and all working files of NONPUBLIC PATIENT LEVEL DATA, OSHPD requires that security measures be evaluated before data is stored on a system. The security requirements below are measures which are expected on a secure system. Additional security requirements for specific system types can be found on the following pages. Researchers that do not maintain their own system should validate security requirements with the system security professionals.

Definitions of the types of systems used are:

1. Standalone Computer – a computer with no communications to external systems
2. Networked Computer – a single computer with external communications (such as Internet), and it is not used as a server
3. Host-based system – a computer or terminal attached to a server where the programs and/or data is maintained on the host computer

The following are found on secured systems:

Software:

- Anti-Virus
- Anti-Spyware (examples of available products include: Adaware™, Spybot™, Pest Control™, Giant™, Symantec 9, or Pest Patrol™)
- No remote access software (i.e., PC Anywhere™, Remote Control™, SNMP, etc.)

Access Control:

- Access must be restricted to the authorized individual(s)
- Password length must be a minimum of eight characters for windows based systems
- Passwords should be a mix of alphanumeric characters and symbols
- Passwords cannot be observable (cannot be read when entered) or recordable (cannot be captured in a key logger or other similar device or system), guessable, shared with others, or stored in a readable format

Physical Environment:

- Monitor must be positioned to prevent others from viewing text on screen
- Printers should be placed in close proximity for quick pickup of printouts
- Password protected screen savers must be used when a computer is in a shared workspace

Data Storage:

- Store removable media (CD-ROM, USB Drive, etc.) in a locked cabinet or drawer
- Data stored on hard drives must be encrypted

Encryption:

- Acceptable encryption standards include Triple-DES; PCP; AES; Windows file encryption system

Recommended Practices for Safeguarding Access to Confidential Data

The following are additional security requirements specific to the type of computer used:

1. Stand-alone Computer

   Software:

   - Anti-Virus and Anti-Spyware scans are required before the CD containing the data is initially accessed

2. Networked Computer

   Software:

   - Anti-Virus continuous scan
   - Anti-Spyware continuous scan
   - Security patches must be kept current (i.e., Microsoft Windows™, Internet Explorer, media players, etc.)

   Hardware:

   - External firewall (such as net gear™, Cisco pix™ or other that is NCSA certified)
   - Host Intrusion System (such as Zone Alarm™) Note: Windows™ firewall does not provide adequate security

   Network:

   - NO WiFi connections

   Back-ups:

   - Backups of the data are to be restricted to the researcher and authorized staff. The backups of the data should be stored separately from the network backups. No data should be stored with the network backups

   Services:

   - Disable all unnecessary services
   - Peer-to-peer services must be disabled (i.e., Kaaza, edonkey, emule, etc.)
   - File sharing must be prevented

   Logs:

   - Must be maintained for use of data
   - Must be maintained for all Read access to data
   - Are to be kept for the entire period of authorization for use of data

3. Host-based System

   Network:

   - Intrusion Detection System
   - Firewall
   - NO WiFi connections
   - Network connections must be isolated and secured

Recommended Practices for Safeguarding Access to Confidential Data

Services:

- Disable all unnecessary services
- Peer-to-peer services must be disabled (i.e., Kaaza, edonkey, emule, etc.)
- File sharing must be prevented

Software:

- Anti-Virus – continuous scan
- Anti-Spyware – continuous scan
- Security Patches must be kept current

Back-ups:

- Backups of the data are to be restricted to the researcher and authorized staff. Ensure that the data is backed up but stored separately from the Host backups. No data should be stored with the Host backups

Logs:

- To be stored on an external system
- Must be maintained for use of data
- Must be maintained for all Read access to data
- Are to be kept for the entire period of authorization to data

Additional Security Guidelines

Acceptable options for data destruction include:

- Use of cross-cut shredder for any hardcopy printouts of any portions of the patient level data
- Shred or break CD-ROM and diskettes into small pieces
- Use of demagnetizer for magnetic media

In the event of a hard drive failure: if the nonpublic patient level data cannot be removed from a hard drive prior to recovery efforts, a confidentiality agreement must be signed with the recovery services before commencing work.

At the conclusion of the project: secure erasure techniques are to be employed to ensure deletion of patient level data. All temporary files containing patient level data must be deleted and a signed notification, listing the procedure used to ensure permanent deletion of all temporary files, sent to OSHPD.

Disclaimer: software products listed are used as examples only. OSHPD does not endorse any of the software products listed.