

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 confidential birth and death data, the Vital Statistics Advisory Committee 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. Principal investigators who do not maintain their own systems should validate security requirements with system security professionals.

Systems are defined as:

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

The following are features of secured systems:

Software:

- Anti-Virus
- Anti-Spyware
- Absence of remote access software

Access Control:

- Must be restricted to authorized individual(s)
- Password length must be a minimum of eight characters for windows-based systems
- Passwords should contain 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, diskette, USB Drive, etc.) in a locked cabinet or drawer
- Data stored on hard drives must be encrypted

Recommended Practices for Safeguarding Access to Confidential Data

Encryption:

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

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

Stand-alone Computer

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

Networked Computer

- Software:
 - o Anti-Virus continuous scan
 - o Anti-Spyware continuous scan
 - o Current security patches on all programs
- Hardware:
 - o NCSA-certified External firewall
 - o Host Intrusion System Note: Windows™ firewall does not provide adequate security

Network: Absence of WiFi Connections

Back-ups:

- Restricted to the researcher and authorized staff
- Stored separately from network backups.
- No data should be stored with network backups

Services:

- Disable all unnecessary services
- Peer-to-peer services disabled
- File sharing must be prevented

Logs:

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

Host-based System

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

Recommended Practices for Safeguarding Access to Confidential Data

- Services:
 - o Unnecessary services disabled
 - o Peer-to-peer services disabled
 - o File sharing must be prevented
- Software:
 - o Anti-Virus – continuous scan
 - o Anti-Spyware – continuous scan
 - o Security Patches must be kept current
- Back-ups:
 - o Restricted to the researcher and authorized staff
 - o Data is backed up but stored separately from host backups.
 - o Data not stored with host backups
- Logs:
 - o Stored on an external system
 - o Maintained for use of data
 - o Maintained for all read access to data
 - o Kept for the entire data authorization period

Additional Security Guidelines

Acceptable options for data destruction include:

- Use of cross-cut shredder for any hardcopy printouts of any portions of non-confidential, individual level data
- Shred or break CD-ROM and diskettes into small pieces (disassemble diskette to cut disk into small pieces)
- Use of demagnetizer for magnetic media.

If non-confidential data cannot be removed from a hard drive prior to recovery efforts in the event of a hard drive failure, a confidentiality agreement must be signed with the recovery services before commencing work.

Secure erasure techniques are to be employed to ensure deletion of identifiable data after the project is concluded.

All temporary files containing identifiable data must be deleted and HIRS must receive a signed notification listing the procedure used to ensure permanent deletion of all temporary files.

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