SAN BERNARDINO COUNTY
Behavioral Health
303 E. Vanderbilt Way San Bernardino | (909) 388-0900
www.SBCounty.gov

Workstation and System Security Policy

Effective Date	10/05/2006	DocuSigned by: Dr. Georgina Yoshioka 7DF8077EFA674B2...
Revised Date	07/24/2024	Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to ensure standardization of the physical attributes of its information systems and related infrastructure to assure the secure maintenance of confidential and protected health information (PHI), and prevent unauthorized access in accordance with Title 45 Code of Federal Regulations (CFR) §164.310 and §164.312(a)(2)(ii) (Health Insurance Portability and Accountability Act (HIPAA) Security Rules).

Purpose

To outline the security measures in place to protect workstations and servers in which confidential and PHI is accessed and stored.

Definition(s)

ePHI: Any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media.

Firewall: A part of a computer system or network which is designed to block unauthorized access while permitting outward communication.

Protected Health Information (PHI): Individually identifiable information relating to the past, present, or future health status of an of an individual that is created, collected, transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare.

Staff Use of System and Privileges

System users that send, receive, store and access ePHI must comply with the DBH **Computer and Network Appropriate Use Policy** (IT5004) which specifies in part:

- Workforce members utilizing DBH systems should have no expectation of privacy, as monitoring of workstations and system access may occur. DBH may log, review, or monitor any data stored or transmitted on its information systems to manage those assets and ensure compliance with County and Department policies, and
- DBH may remove or deactivate any workforce member's privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

Continued on next page

System Security

All workstations used to access, transmit, receive, or store ePHI (electronic PHI) must comply with the **Computer and Network Appropriate Use Policy** (IT5004). If any of the policy requirements are not supported by the workstation operating system or system architecture, one of the following steps must be taken:

- The system must be upgraded to support all security measures;
- An alternative security measure must be implemented and documented, or
- The workstation shall not be used to send, receive, or store ePHI.

Server Security

DBH Information Technology (IT) is responsible for ensuring all servers used to access, transmit, receive or store ePHI are secured in accordance with this policy.

The following server security features/actions apply:

- Must be located in a physically secure environment;
- System administrator account must be password protected;
- Network drives storing ePHI or temporary files must be secured with 128-bit encryption;
- User identification and password authentication mechanism must be implemented to control user access to the system;
- Security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied in accordance with the severity of the vulnerability corrected;
- Must be located on a secure network with firewall protection;
    - If for any reason the server must be maintained on a network that is not secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity, and
- Promptly disable all unused or unnecessary applications/programs.

Infrastructure Security

DBH IT is responsible for ensuring all infrastructure equipment used to access, transmit, receive or store ePHI is stored in accordance with this policy.

The following infrastructure security features/actions apply:

- Must be in a physically secured environment know as Main Distribution Frame (MDF), Intermediate Distribution Frame (IDF), or commonly referred to Communications Rooms.
- Communication Rooms must be secured and accessed by authorized DBH IT staff only.

Continued on next page

Infrastructure Security, continued

- Non-DBH IT staff requiring access to communications room for business purposes must be accompanied by DBH IT staff at all times.
- Non-DBH IT staff requiring access to Communications Rooms must include the reason for accessing and have prior approval from the IT Senior Program Manager (SPM) or Deputy Director (DD) overseeing IT.
- Access to Communications Rooms provided to non-DBH IT staff will be logged in by accompanying DBH IT staff and reported to the IT SPM monthly.

Desktop Security

DBH IT is responsible for ensuring each desktop system used to access, transmit, receive or store ePHI is secured in accordance with this policy.

The following desktop security features/actions apply:

- User identification and password authentication mechanism must be implemented to control user access to the system;
- All desktop hard drives must be secured with 128-bit encryption;
- Security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on severity of vulnerability corrected;
- System virus detection must be implemented including assurance of virus detection software maintenance and updates;
- All unused or unnecessary applications/programs shall be promptly disabled;
- Automatic logoff or inactivity timeout mechanism shall be implemented as specified in the Logoff Requirements section of this policy, and
- Workstation screens or display shall be situated in a manner that prohibits unauthorized viewing or shall utilize a screen guard or privacy screen.

Continued on next page

Logoff Requirements

To ensure access control to all servers and workstations that transmit, receive, or store ePHI, the following requirements apply:

- Servers, workstations, or other computer systems containing ePHI must employ inactivity timers or automatic logoff mechanisms;
- Aforementioned systems must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity;
- If a system requires the use of an inactivity timer or automatic logoff mechanism, but does not support an inactivity timer or automatic logoff mechanism, one of the following must be implemented:
  - System must be upgraded to support the minimum HIPAA Security Automatic Legoff procedures;
  - System must be moved into a secure environment, or
  - ePHI must be removed and relocated to a system that supports the minimum requirements.

Before leaving a server, workstation, or other computer system unattended, system users shall:

- Lock or activate the systems Automatic Logoff Mechanism (e.g. CTRL, ALT, DELETE and Lock Computer), or
- Logout of all applications and database systems containing confidential information.

Tracking Requirements

To ensure that PHI remains secure, IT will maintain current lists of all of the following items:

- Devices throughout DBH that access PHI and their locations;
- Authorized users within DBH that access PHI, and
- Approved applications for use on devices and that IT specialists work with.

Consequences of Violations

Staff violations of DBH systems as described above or in other County policies will be subject to disciplinary action, up-to and including termination of employment.

Related Policy or Procedure

DBH Standard Practice Manual and Forms:

- Privacy Incident Policy (COM0944)
- Computer and Network Appropriate Use Policy (IT5004)

Reference(s)

- Code of Federal Regulations, Title 45, Parts 160 and 164,
- Code of Federal Regulations, Title 42, Part 512, §512.275