County of San Bernardino
Department of Behavioral Health

Workstation and System Security Policy

Effective Date	10/5/06	
Approval Date	10/5/06	**Allan Rawland, Director**

Policy

The Department of Behavioral Health (DBH) will standardize the physical attributes required to protect information systems and related infrastructure from unauthorized access in accordance with HIPAA Security Rules 164.310 and 164.312(a)(2)(ii) to protect the availability, confidentiality, and integrity of client and departmental confidential information.

Purpose

To describe the physical attributes of the surroundings of a system or class of system that can access or contains ePHI and establish guidelines which defines the proper functions and manner in which system users are to perform those functions.

General Information

System users that send, receive, store and access ePHI must comply with the Behavioral Health Computer and Network Appropriate Use Policy.

Staff Use of System and Privileges

Monitoring of workstation use

Staff utilizing DBH systems should have no expectation of privacy. DBH may log, review, or monitor any data stored or transmitted on its information systems to manage those assets to ensure compliance with the departments policies.

Removal of staff privileges

DBH may remove or deactivate any staff'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.

System Security

Each workstation that is used to access, transmit, receive or store ePHI must comply with the Computer and Network Appropriate Use Policy. 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 of the following security measures.
- An alternative security measure must be implemented and documented.
- The workstation must not be used to send, receive, or store ePHI.

Server Security

Information Technology is responsible to ensure that all servers used to access, transmit, receive or store ePHI are appropriately secured in accordance with this policy.

- Servers must be located in a physically secure environment
- The system administrator account must be password protected
- A user identification and password authentication mechanism must be implemented to control user access to the system
- A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
- Servers 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
- All unused or unnecessary services shall be disabled

Desktop Security

Information Technology is responsible to ensure that each desktop system used to access, transmit, receive or store ePHI is appropriately secured in accordance with this policy.

- A user identification and password authentication mechanism must be implemented to control user access to the system
- A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
- A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date
- All unused or unnecessary services must be disabled
- An automatic logoff or inactivity timeout mechanism must be implemented
- The workstation screen or display must be situated in a manner that prohibits unauthorized viewing
- The use of a screen guard or privacy screen is recommended

Logoff Procedures

To ensure that access to all servers and workstations that access, transmit, receive, or store ePHI is appropriately controlled, the following procedures must be followed:

Automatic Logoff

- Servers, workstations, or other computer systems containing ePHI must employ inactivity timers or automatic logoff mechanisms

- The 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 procedures must be implemented:
    - The system must be upgraded to support the minimum HIPAA Security Automatic Logoff procedures
    - The system must be moved into a secure environment
    - ePHI must be removed and relocated to a system that supports the minimum requirements

Logging off the system

If a server, workstation, or other computer system is unattended:

- System users must 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

---

Consequences of Violations

Staff violations of DBH systems as described above or in other County policies will be subject to disciplinary action that can include termination of employment.

Related Policies

Computer and Network Appropriate Use Policy