County of San Bernardino
Department of Behavioral Health

Remote Access Policy

Effective Date 01/29/2007
Revision Date 10/26/2010

Allan Rawland, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to standardize the physical attributes necessary to control access to systems and data that may contain client Personal Health Information (PHI) and/or Personally Identifiable Information (PII) and other departmental confidential data, to ensure its continued availability, confidentiality and integrity.

Purpose

For Information Technology (IT) to fulfill its responsibility for ensuring proper steps are taken to minimize, control and rectify any unauthorized access to DBH systems. To establish guidelines and define functions to be performed, the manner in which such functions are to be performed, and the physical attributes for controlling remote access to DBH systems and data by business associates, vendors and workforce members.

Authorization

IT may authorize remote access to County and/or DBH electronic data systems to:

- Allow vendors the capability to perform system software, application software and infrastructure maintenance
- Provide contract agencies the ability to complete data entry or file uploads
- Provide the department's business associates the capability to receive or deposit specific data identified in a "scope of work"

Remote Access Requirements

The following requirements apply to remote access:

- All persons accessing the network, regardless of origin, must have a unique User Identification (User-ID) and complex password authorized and configured by IT specifically for that purpose
- All persons accessing data that may contain client PHI and/or PII must have completed the County/DBH HIPAA Privacy/Security and application training requirements. **Vendors whose systems are in use by DBH are excluded from this requirement**
- All remote connections must be:
  - Approved and controlled by IT and be assigned a unique User-ID and complex password
  - Authorized, authenticated and secured before access to the network/system is granted

Continued on next page

Remote Access Policy, Continued

Remote Access Requirements (continued)

- Remote access methods are:
  - Virtual Private Network (VPN)
  - Telnet
  - DEC NET

Intrusion Detection Software

County Network:

- The County network is protected by a "Firewall" that prohibits users and or transmissions from gaining access to the various systems and data is maintained by the Network Services Division (NS) within the Information Services Department (ISD)
- The Core Services and Security Division (CSSD) within ISD maintains a series of intrusion detection software applications monitored on a twenty-four (24) hour basis to identify and report any unauthorized or suspicious access attempt
- CSSD will immediately contact the owner of an impacted system should an unauthorized or suspicious attempt to gain entry be detected
- IT, working in collaboration with CSSD, will take appropriate action to mitigate and resolve further unauthorized activity of this type

County E-mail System:

- CSSD is charged with maintaining the email server data and preventing unauthorized or suspicious access by:
  - Installing, monitoring and maintaining intrusion detection software
  - Encrypting all data that resides on e-mail servers
  - Quarantining suspected files that may contain unauthorized data and/or viruses
  - Escalating security and or virus related issues to potential departments that may be affected
- IT working in collaboration with ISD, will take appropriate action to mitigate and resolve all virus contamination that has impacted the department's LAN network

Application Systems:

- The Technical Operations Division (TSO) within ISD is charged with installing, monitoring and maintaining the intrusion detection software that monitors and reports any unauthorized access attempts impacting the DEC/VMS and SQL server environment on a twenty-four (24) hour basis
- Software logs are reviewed on a daily basis and suspected concerns are escalated to the TSO management team and to potential departments that may be affected

Continued on next page

Remote Access Policy, Continued

Intrusion Detection Software (continued)

- IT working in collaboration with TSO, will take appropriate action to mitigate and resolve unauthorized activity
- ISD's NS and CSSD will be notified if unauthorized activity needs to be escalated for resolution

Violations

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

References

Code of Federal Regulations 42, Part 431.300, Section 2.1 et seq.
Code of Federal Regulations 45, Parts 160 and 164.
California Civil Code 56 et seq. (The Confidentiality of Medical Information Act)
California Health and Safety Code (Information Practices Act of 1977), Section 1798
et seq., Section 123100 et seq. (Client Access to Health Records)
California Welfare and Institutions Code, Sections 5328 et seq., 14100
Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)
Department of Behavioral Health Medi-Cal Privacy and Security Agreement

Related Policy or Procedure

County of San Bernardino Policy Manual 14-01: Electronic Mail (E-mail) Policy
County of San Bernardino Policy Manual 14-04: Internet/Intranet Use Policy
County of San Bernardino Policy Manual 16-02: Protection of Individually Identifiable Health Information
County of San Bernardino Policy Manual 16-02SP1: Protections of Individually Identifiable Health Information
DBH Standard Practice Manual IT5003: Internet Account Policy
DBH Standard Practice Manual IT5004: Computer and Network Appropriate Use Policy
DBH Standard Practice Manual IT5005: Electronic Mail Policy
DBH Standard Practice Manual IT5006: Remote Access Policy
DBH Standard Practice Manual IT5008: Device and Media Controls Policy
DBH Standard Practice Manual IT5009: User I.D. and Password Policy