303 E. Vanderbilt Way San Bernardino | (909) 388-0900
www.SBCounty.gov

Remote Access Policy

Effective Date 01/29/2007
Revised Date 09/20/2021

Veronica Kelley, DSW, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to ensure secure systems are in place for authorizing remote access to the DBH network for approved County employees and authorized third parties who have an identified need for such access and demonstrate compliance with DBH's established safeguards.

Purpose

The purpose of this policy is to provide guidelines for remote access and Virtual Private Network (VPN) connections to the County network. The County's VPN is designed to provide secure encrypted access to network resources and ensure proper steps are taken to prevent and rectify any unauthorized access to DBH systems.

Definition(s)

Electronic Protected Health Information (ePHI): Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Firewall: A set of hardware and/or related programs providing protection from attacks, probes, scans and unauthorized access by separating the internal network from the Internet.

Privileged Access Controls: Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permissions, and role-based access controls.

Remote Access: The ability to gain access to the DBH network from outside the network perimeter. Common methods of communication from the remote computer to the County's network include, but are not limited to Virtual Private Networks (VPN), web-based Transport Layer Security (TLS) portals, and other methods which employ encrypted communication technologies.

Role-Based Access: Access controls based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on only those privileges which are essential to perform their intended function.

Teleworker: An individual working at home or other approved location away from the regular work site on an established work schedule using a combination of computers and telecommunications.

Continued on next page

Remote Access Policy, Continued

Definition(s), continued

Virtual Private Network (VPN): A private network that connects computers over the Internet and encrypts their communications.

Web-based Portal: A secure website offering access to applications and/or data without establishing a direct connection between the computer and the hosting system.

Workforce Members: Employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Authorization

Remote access is strictly controlled and made available only to workforce members with a defined business need, at the discretion of the workforce member's manager, and with approval by the DBH-Information Technology (IT) Manager or designee.

- The workforce member is responsible for adhering to all DBH policies and procedures, including avoiding engaging in illegal activities, and not using remote access for interests other than those for San Bernardino County.
- Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or written agreement with DBH which clearly defines the type of remote access permitted as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by DBH-IT and/or legal department before remote access will be permitted.

Remote Access & VPN Requirements

Remote Access Equipment:

Devices may only access the county network and data through the Internet using a Transport Layer Security (TLS) and Virtual Private Network (VPN) connection.

- Remote users will be allowed access through the use of DBH County equipment or through the use of the workforce member's personal computer system, provided it meets the minimum standards developed by DBH.
- Remote users utilizing personal equipment, software, and hardware are:
  - Responsible for remote access, DBH will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss;
  - Responsible for remote access used to connect to the network and meeting DBH County requirements for remote access, and
  - Responsible for the purchase, setup, maintenance or support of any equipment not owned by or leased to DBH.

Continued on next page

Remote Access Policy, Continued

Remote Access & VPN Requirements continued

- Continued service and support of DBH owned equipment is to be completed by IT workforce members. Troubleshooting of telephone or installed broadband circuits is the primary responsibility of the remote access user and their Internet Service Provider (ISP). It is not the responsibility of DBH to work with ISPs on troubleshooting problems with telephone or broadband circuits not supplied and paid for by DBH.

Security & Privacy:

- Only authorized remote access users are permitted remote access to any DBH computer system, network, and/or information, and must adhere to all DBH policies.
- It is the responsibility of the remote access user, including Business Associates, contractors and vendors, to log-off and disconnect from the DBH network when access is no longer needed to perform job responsibilities.
  - Remote access users shall lock the workstation and/or system(s) when unattended to ensure no other individual is able to view or access any ePHI or sensitive information,
  - Remote access users are automatically disconnected from the DBH network when there is no recognized activity for 30 minutes,
  - It is the responsibility of remote access users to ensure unauthorized individuals do not access the network. At no time will any remote access user provide their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password,
  - Remote access users must take necessary precautions to secure all of DBH equipment and proprietary information in their possession;
- Copying of confidential information, including ePHI, to personal media is strictly prohibited, unless prior approval is granted in writing;
- DBH-IT maintains logs of all activities performed by remote access users while connected to the DBH network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity;
- Users may only send ePHI in an encrypted manner approved by DBH;
- All persons accessing data that may contain client ePHI 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 DBH-IT and be assigned a unique User-ID and complex password in accordance with the User- I.D. and Password Policy (IT5009), and
  - Authorized, authenticated and secured before access to the network/system is granted.

Continued on next page

Remote Access Policy, Continued

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 County Innovation and Technology Department (ITD);
- ITD 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;
- ITD will immediately contact the owner of an impacted system should an unauthorized or suspicious attempt to gain entry be detected, and
- DBH-IT, working in collaboration with ITD, will take appropriate action to mitigate and resolve further unauthorized activity.

County E-mail System:

- ITD 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, and
  - Escalating security and or virus-related issues to potential departments that may be affected.
- DBH-IT working in collaboration with ITD will take appropriate action to mitigate and resolve all virus contamination that has impacted the department's Local Area Network (LAN).

Application Systems:

- DBH-IT working in collaboration with ITD is charged with installing, monitoring and maintaining the intrusion detection software that monitors and reports any unauthorized access attempts impacting the County Network on a twenty-four (24) hour basis.
- Software logs are reviewed on a daily basis and suspected concerns are escalated to the DBH-IT Security Team and to potential departments that may be affected.

Violations

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

Continued on next page

Remote Access Policy, Continued

Related Policy or Procedure

County of San Bernardino Policy Manual
- Electronic Mail (E-mail) Policy (09-01)
- Internet/Intranet Use Policy (09-04)
- Non-Public Personally Identifiable Information (14-02)
- Uses and Disclosures of Protected Health Information (14-03SP06)

DBH Standard Practice Manual
- Internet Account Policy (IT5003)
- Computer and Network Appropriate Use Policy (IT5004)
- Electronic Mail Policy (IT5005)
- Device and Media Controls Policy (IT5008)
- User I.D. and Password Policy (IT5009)

Reference(s)

- 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
- Department of Behavioral Health Medi-Cal Privacy and Security Agreement
- Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)