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

DBH-IT Data Encryption Policy

DocuSigned by:
Dr. Georgina Yoshioka, Interim Director
7DF8077EFA674B2...

Approved Date	2/28/2022	
Effective Date	2/28/2022	Georgina Yoshioka, DSW, MBA, LCSW, Interim Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to ensure encryption safeguards and integrity controls are in place for protection and safeguarding of electronic protected health information (PHI), and highly sensitive information during transmission and while stored on all DBH laptops, workstations, servers and portable drives.

Purpose

To provide instruction to the DBH-IT workforce for ensuring data containing confidential and protected information is stored, transferred and transmitted in accordance with the Health Insurance Portability and Accountability Act of 1996, Security Rule (HIPAA), including addressing encryption requirements for maintaining the confidentiality and integrity of DBH sensitive data. The technical standards governing security are derived from Generally Accepted Security Principles and Practices for Securing Information Technology Systems, published by the National Institute of Standards and Technology (NIST).

Definition(s)

Advanced Encryption Standard (AES): A symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Electronic protected health information (ePHI): PHI that is produced, saved, transferred or received in an electronic form.

Encryption: Converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

File Encryption: The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided.

Folder Encryption: Encryption of individual folders on a storage medium and permitting access to the encrypted files within the folders only after proper authentication is provided.

Full Disk Encryption: Encryption of all data on the hard drive used to boot a computer, including the computer's operating system. Access is permitted to the data only after successful authentication with the full disk encryption product.

Continued on next page

DBH-IT Data Encryption Policy, Continued

Definition(s), continued

Hardware and Electronic Media: All stationary and portable hardware, devices, and storage that access or contain sensitive or highly sensitive information from DBH's network. This includes, but is not limited to:

- Servers, workstations, and laptops
- Hard disk drives (fixed or removable)
- Implantable and wearable devices
- Smartphones, tablets and Mp3 players
- USB portable drives (flash drives)
- SD cards and other removable memory cards
- CDs and DVDs
- Backup tapes and related media

Highly Sensitive Information: Protected health information, personally identifiable information (PII) or any information that, if lost, corrupted, disclosed to or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may (i) violate federal, state, and/or local law, (ii) cause significant harm, injury, or damage to another person or entity, or (iii) cause financial loss to another person or entity.

Encryption Requirements

The DBH Information Technology Department (DBH-IT) shall:

- Implement strong encryption safeguards to prevent compromise of highly sensitive information and ePHI if accessed without proper authorization, and
- Specify use of industry protocols to facilitate exchange of information between authorized business partners and others authorized to access the information.

Any transfer of unencrypted DBH highly sensitive information or ePHI must take place through an encrypted channel established by DBH-IT.

E-mail Encryption

- If data itself is encrypted it may be transmitted through either encrypted or unencrypted channels.
- All email communications containing **DBH highly sensitive information or ePHI** to email addresses outside of the County Network (sbcounty.gov) must use an encrypted channel in accordance with the DBH Electronic Email Policy and use Federal Information Processing Standards (FIPS) 140-2 certified algorithm which is 128bit or higher, such as AES.

Continued on next page

DBH-IT Data Encryption Policy, Continued

Encryption Requirements, continued

Data Transmission Encryption (Devices and Media):

- **Data must be encrypted whenever DBH highly sensitive information or ePHI is placed on a portable medium such as a CD, DVD, or portable drive to facilitate a physical transfer, either entirely within DBH or between DBH and an authorized 3rd party.**
- All data transmissions of highly sensitive information or ePHI outside the secure internal DBH network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing ePHI can be encrypted. This requirement pertains to any type of highly sensitive information or ePHI in motion such as website access, file transfer, and e-mail.

If a wireless network is used to transmit ePHI, the following conditions must be met:

1. The connection through the wireless network must utilize an authentication mechanism to ensure wireless devices connecting to the network are authorized; **and**
2. The connection through the wireless network must utilize an encryption mechanism for all transmissions over the network.
    1) If transmitting ePHI over a wireless network not utilizing an authentication and encryption mechanism, the ePHI shall be encrypted before transmission.

Data Storage Encryption:

- All electronic files that contain DBH highly sensitive information or ePHI must be encrypted when stored on any hard drive, removable media or portable device (i.e. USB thumb drives, flash drives, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm that is 128bit or higher, such as AES.
- DBH highly sensitive information or ePHI stored on servers must have sufficient file, folder or full disk encryption to protect the data.

Remote Access Encryption:

- When accessing the DBH secure network an encryption communication method, such as Virtual Private Network (VPN), shall be used in accordance with DBH Remote Access Policy (IT5006). DBH-IT must evaluate department products used to manage information under their control to ensure strong password encryption security policies are enabled.

Continued on next page

DBH-IT Data Encryption Policy, Continued

Encryption Requirements, continued

Portable Device Encryption:

- DBH-IT uses full disk encryption as the method for encrypting laptop PC's and other portable devices, such as cell phones. Full disk encryption ensures everything on the hard disk, including the operating system, applications, and data files are encrypted. Any encryption product that uses a FIPS 140-2 certified algorithm which is 128bit or higher (e.g. BitLocker) is acceptable. The selection, implementation and use of encryption products will be determined by the DBH-IT Director or designee.

Privacy or Security Incident

In the event of an attempted or successful unauthorized access, use, disclosure, modification, or destruction of ePHI or other highly sensitive data, the incident must be promptly reported to the Office of Compliance in accordance with the Privacy and Security Incident Policy.

Related Policy or Procedure

DBH Standard Practice Manual:

- Electronic Transfer of Client Protected Health Information- Internet and Intranet Policy (COM0909)
- Data Integrity Policy (COM0925)
- Privacy and Security Incident Policy (COM0944)
- Electronic Email Policy (IT5005)
- Remote Access Policy (IT5006)
- Device and Media Controls Policy (IT5008)

Reference(s)

Health Insurance Portability and Accountability Act, Privacy Rule
National Institute of Standards and Technology