DAVIS BEHAVIORAL HEALTH
Community • Commitment • Change

Policies & Procedures

SECURITY OF PHI:

TECHNICAL SAFEGUARDS

Section: HIPAA

Pages: 2

Subject: Security of PHI: Technical Safeguards

Effective Date:

Revision Date: 05/10/2023

POLICY

Technical safeguards shall be implemented to secure protected health information (PHI) and patient identifying information (PII) in all formats from unauthorized access at all times and to protect the information from damage, loss, alteration, tampering, and fraudulent use or disclosure.

PROCEDURES

1. Access Control *(45 CFR 164.312(a)(1) and (2)(i – iv))*

   A. Unique user identification

      1) They said to just repeat this line. DBH shall assign a unique name and/or number for identifying and tracking user identity.

   B. Emergency Access procedure

      1) See Contingency Plan section of "Security of PHI: Administrative Safeguards" policy.

   C. Automatic Logoff

      1) Access to the network is limited by password protected personal accounts assigned to individuals who are specifically identified and authenticated by the supervisor and Human Resources staff on the Personnel Action Form (PAF). Access is granted for defined work- related purposes and for defined periods of time.

   D. Encryption and Decryption

      1) Email. The user has an option to select an alternate signature block to encrypt the message as soon as email goes outside of DBH. Any subsequent conversation with the recipient in that email chain is also encrypted. Further, an algorithm searches emails being sent outside the agency for PHI. The algorithm may include PHI indicators such as key words, social security numbers, etc. If indicators are located, the system flags the email and submits it to IT. The email is not released until reviewed and approved by IT reviews.
      2) Medical records. PHI is encrypted by the third-party vendor. The vendor is accountable to DBH via its Business Associate Agreement.

3) Text messaging. DBH staff shall only communicate via text or instant messaging if the communication in no way shares PHI or otherwise identifies an individual as a client of Davis Behavioral Health.

2. Audit Controls *(45 CFR 164.312 (b))*

   A. Procedural mechanisms that record and examine activity

1) In the electronic medical records system, every click is logged and tracked to the user. Assigned administrators, such as the Security Officer have been given rights to view reports on user activity.
2) The firewall provides tracking of any attempted breaches.

3. Integrity *(45 CFR 164.312(c))*

A. Authentication

1) Each client of DBH is assigned to a program in the electronic medical records system. Users are granted job-specific access and do not have rights to view PHI of clients in other programs. Users have read/write access for their own clients but, once data is saved, they do not have rights to alter or destroy data. If a user needs to correct an input error, the user shall contact the assigned administrator to make the correction.

4. Person or Entity Authentication *(45 CFR 164.312(d))*

Each user has a unique name and/or number and each login is password-protected.

References: *HIPAA Regulations incorporated above*