DAVIS BEHAVIORAL HEALTH
Community · Commitment · Change

Policies & Procedures

SECURITY OF PHI:

ADMINISTRATIVE SAFEGUARDS

Section: HIPAA

Pages: 4

Subject: Security of PHI: Administrative Safeguards

Effective Date: 08/2017

Revision Date: 05/10/2023

POLICY

Administrative 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. Workforce Security *(45 CFR 164.308(3)(a)(i) and (ii)(A – C); 164.308(4)(a)(i) and (ii)(B – C))*

   A. New employees

      1) Upon hiring, the new employee's supervisor will submit a signed Personnel Action Form (PAF) to the Human Resources Office, requesting job-specific access to the network. Human Resources will complete the approval of the PAF and will generate a support ticket for IT staff to complete the action.
      2) Job-specific access will be locked down to information that is relevant to the employee's position, including access to department information, shared folders, email distribution lists, and medical records.

   B. Change of Position or Termination of Employment

      1) Upon change of position within DBH or termination of employment from DBH, the employee's supervisor will fill out and sign the relevant section of the PAF and submit it to Human Resources which will then complete the form and generate a support ticket for IT staff to take the following action:
         a. For change of position, IT will terminate the employee's access to any information that is no longer relevant to the new job position and will initiate job-specific access to relevant information.
         b. For termination of employment, IT will immediately terminate the employee's access to the network. Supervisors are also required to collect keys and other access devices if the employee's job duties

include authorized access to any area where health information is stored or used.

2. Access Authorization *(45 CFR 164.308(a)(4)(i) and (ii)(B – C))*

A. Password Protection

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 PAF. Access is granted for defined work-related purposes and for defined periods of time. The PAF shall provide information of individuals who have been given access to any data and shall include, at minimum:

   a) The individual's name and work responsibilities

   b) The date access was given, and the reason access was given to the data

   c) The individual's assigned account information

   d) The date access was terminated and the reason for termination

2) Employees shall log in to the network with a protected password. Three incorrect password attempts will result in the person being locked out from another attempt for 15 minutes. IT staff may be contacted if earlier login is necessary.

B. Network Protection

1) As a new employee is issued a computer, it is automatically updated upon connection to the system network. The connection includes Unified Threat Management (UTM) which provides, but is not limited to, security functions such as:

a) Port blocking

b) Content Filter

c) Deep packet inspection

d) Intrusion Prevention

3. Access establishment and modification *(45 CFR 164.308(a)(4)(ii)(C))*

A. Review and modification of user's right to access

1) A user's right to access a workstation, transaction, program, or process is established, reviewed, and documented through the Human Resources Personnel Action Form and process described in Sections 1 and 2 above.

4. Security Incidents *(45 CFR 164.308(a)(6)(i))*

   A. Preventing, detecting, containing, and correcting security breaches and violations.

      1) Security incidents include viruses, worms, hoax e-mails, hacking, altered data, deliberate disruptions of service, and other unauthorized use of computer accounts and systems.
      2) Quarterly, IT staff will run a HIPAA-compliance audit tool (such as "Network Detective" by Rapid Fire Tools) and will provide the results of the audit to the DBH Executive Leadership Team (ELT).
      3) Security incidents involving inappropriate use or disclosure of protected health information shall be reported to the Security Officer immediately.

         a) The Security Officer will report known and suspected security incidents to the appropriate Program Manager for investigation, repair, restoration, and disciplinary action, as necessary.
         b) The Security Officer will document the outcome and report the results to ELT.

5. Contingency Plan *(45 CFR 164.308(a)(7)(i) and (ii)(A – E))*

   A. Data Backup Plan

      1) DBH maintains two identical data centers, including servers and storage devices, in separate locations on the DBH campus. These data centers continually replicate to each other. Damage or malfunction in one center is backed up by the other without disruption in system function or service.
      2) All data maintained in the above two centers shall also replicate to a third-party cloud service, such as Microsoft Azure.
      3) All user account information and permissions are replicated to a 3rd location on the DBH campus.

   B. Disaster Recovery Plan

      1) As described in *Section 5(A)(1)* above, in the event of damage or malfunction in one of the two data centers, the other data center will continue to perform without disruption to function or service.
      2) In the event that both data centers maintained on campus are damaged or otherwise rendered unusable (e.g., fire, flood, earthquake), data shall be recovered through the use of third-party cloud service.

   C. Emergency Mode Operation Plan

      1) In addition to the back-up procedures described above, email service shall be hosted by an off-site third-party service, such as Microsoft 365, to enable continuation of business processes.
      2) Medical records shall be supported by an off-site, third-party vendor, such as Credible, to enable continuation of business processes.

D. Testing and revision procedures

1) At least monthly, IT staff shall re-boot servers to test and demonstrate continuity. Any issues and a plan of corrective action shall be reported to ELT.

E. Data Criticality Analysis –

In the event of system failure, IT staff will prioritize the following based on their level of importance for continued business operations:

1) Power/Internet. DBH shall have two lines, such as Comcast and Centricom, to provide continual access. Access may also be gained via the LTE Broadband Card or "mobile hotspot." The two data centers will continue to operate on battery backup as IT staff works to restore power. In the event of failure of the data center battery backup, laptop computers may also be used on battery, as needed, to provide emergency access to medical records and email, operated by off-site, third-party providers.
2) Medical Records and Email. Once power is restored, all medical records and emails shall be again available to all staff.
3) Servers. IT staff shall then restore server functionality, which will once again provide staff with access to documents, shared folders, etc.

6. Sanctions *(45 CFR 308(a)(1)(ii)(C))*

A. Any member of the workforce who fails to comply with DBH Security policies and procedures shall be referred by his/her supervisor to Human Resources for investigation.

References: *HIPAA Regulations cited above*

See also Risk Management-HIPAA Policy.