Policies & Procedures

SECURITY OF PHI:

PHYSICAL SAFEGUARDS

Section: HIPAA

Pages: 2

Subject: Security of PHI: Physical Safeguard

Effective Date: 08/2017

Revision Date: 05/10/2023

POLICY

Physical 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. Facility Access Controls *(45 CFR 164.310(a)(1) and (2)(i – iv))*

   A. Contingency Operations

      1) Job-specific authorization (by key, badge or biometrics) shall be approved by Human Resources to enable such authorized individuals, in the event of an emergency and/or to restore lost data, to immediately access the secured, locked rooms where servers and units are maintained.

   B. Facility Security Plan

      1) In the absence of job-specific authorization described above, no individual shall access the secure storage areas.
      2) No items other than approved IT equipment shall be stored in the secure areas. Any request to store items in these areas must be approved by ELT.

   C. Access Control and Validation Procedures

      1) Facilities. Access to the secure storage areas shall be limited to the job-specific authorization described above. No visitors shall enter the secure area unless accompanied at all times by an individual with approved access.
      2) Software. Any new piece of software shall be test controlled first. Once testing is complete, the software is rolled out to all users. Only administrators have rights to install software.

   D. Maintenance Records

      1) A request for maintenance to the facility may be generated by any staff

member via the support ticket system. IT staff forwards the ticket to the Maintenance Department to take action. Upon completion of repairs or modifications, the ticket is closed and the results documented.

2. Workstation Use *(45 CFR 164.310(b))*

   A. Physical attributes of workstation

      1) For employees who work in private offices, each computer and work station shall be positioned in a manner that PHI and PII are not viewable by visitors if possible. When the employee is away from the office, access shall be protected by password and automatic logoff as described in the Administrative Safeguards policy.
      2) For employees who work in common areas, such as front desk staff and medical assistants, the supervisor shall generate a support ticket to request IT staff to place a physical screen/barrier around the monitor which will inhibit viewing by any individual other than the employee seated directly in front of the screen.

3. Device and Media Controls *(45 CFR 164.310(c)(2)(i – iv))*

   A. Disposal

      1) DBH shall contract with a certified destruction facility to provide the service of destroying hard drives. The company shall provide documentation of the destruction.

   B. Media re-use

      1) When an employee desires to change an office and computer or other device, the supervisor will fill out the relevant section of the Personnel Action Form (PAF) and submit it to Human Resources. Upon completion and approval of the PAF, Human Resources will generate a support ticket for IT staff to take the following action:
         a. Remove the device from the employee's former office.
         b. Verify and complete backup of any data on the device.
         c. Utilize data destruction software, such as DriveWipe, that is certified by the U.S. Department of Defense.

   C. Accountability

      1) See "Purchasing, Inventory & Installation of IT Equipment" policy.
      2) DBH shall implement software approved by IT and the Executive Leadership Team (ELT) to track security and location of assets.

   D. Data backup and storage

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

References: *HIPAA Regulations incorporated above*