Policy Number: HC-22	Page: 1	Of: 2
Title: policies for executive management & HIPAA privacy/security officer		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) HIPAA SECURITY POLICIES--POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA PRIVACY/SECURITY OFFICER

Security Management Process

HCBDD will appoint a HIPAA Privacy/Security Officer. The HIPAA Privacy/Security Officer will orchestrate the board's security management process.

Audience

Executive Management

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(2)

OAC § 5123:2-1-02(I)(7) appointment of person responsible for ensuring the safekeeping of records and securing them against loss or use by unauthorized persons.

REFERENCES

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, 2012

NIST SP 800-53, Security Self-Assessment Guide for Information Technology Systems, 2010

Center for Internet Security at www.cisecurity.org

1) **The Superintendent will designate a HIPAA Privacy/Security Officer**. The job responsibilities for this individual are detailed in Appendix C – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer. The HIPAA Privacy/Security officer will assume the duties detailed in OAC § 5123:2-1-02(I)(7)(a)(5), which include overall responsibility for safekeeping of all records, electronic and paper. Documentation of the designation of the HIPAA Security Officer will be retained with other HIPAA-mandated designations per Policy 1330 HIPAA Assignments and Documentation.
2) **The HIPAA Privacy/Security Officer will be responsible for security management process**. This will include:
    a) **Security Team**. The HIPAA Privacy/Security Officer may issue a request to the Superintendent to appoint a Security Team consisting of managers representing the different functional areas and facilities maintained by the board. The Security Team's charter would be defined by the board, to include assessing risks,

recommending and implementing appropriate technical capabilities, drafting and deploying appropriate security policies and procedures, and periodically validating their effectiveness.

b) **Computer Security Risk Assessment**. The Risk Assessment is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the board. The Computer Security Risk Assessment will be handled as follows:
   i) The county board will use the risk assessment methodology detailed in NIST SP 800-30 (2012).
   ii) The results of this assessment shall be documented and maintained for 6 years.
   iii) The Risk Assessment shall be updated on an annual basis.

c) **Manage IT Infrastructure, Create and Deploy Security Policies**. On an ongoing basis, implement and maintain the IT infrastructure, create Security Policies and Procedures, and deploy them. More specifically, he/she will:
   i) Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices.
   ii) Prepare recommendations for the Superintendent for approval by the board including implementation of new and updated policies, acquisition of technical security measures, or physical security measures. The Board shall have final authority on risk management decisions.
   iii) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level so as to comply with HIPAA regulations.
   iv) Train board staff regarding compliance.
   v) Monitor Board compliance with the information security policies, and take action as appropriate based on this monitoring.

d) **Information System Inventory**. The HIPAA Privacy/Security Officer and/or Security Team shall maintain an inventory of the hardware, software and networking infrastructure.
   i) Content of Inventory:
      1) Hardware inventory will document all servers, routers and other networking equipment, desktop computers, laptops, smartphones and other portable computing devices, external disk drives, and USB flash drives. Inventory will include physical location, primary user, manufacturer / model / serial number.
      2) Network infrastructure documentation will include network topology and all other information necessary to recreate the network in the event of a catastrophic event.
      3) Software inventory will include hardware installed on, Software manufacturer, program name, version number, license/serial number and date.
   ii) Update frequency. This inventory should be updated on an ongoing basis with a physical inventory no less frequent than annually for mobile devices.
   iii) Network Monitoring. (Optional Best Practice.) Network access monitoring may be performed to validate that devices which access the network are included in the inventory. Corrective action should be taken when an unknown device appears.
   iv) Backup copy. A copy of this inventory shall be maintained off-site to insure availability in the event of a fire or other disaster.