

Wood County Board of Developmental Disabilities


POLICY

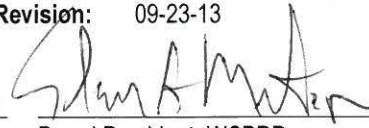
Policy #: 01-ALL-ALL-0161
Effective Date: 04-20-06
Person Responsible: Human Resources Coordinator

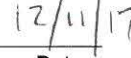
Subject: HIPAA Security
Last Revision: 09-23-13

Approvals/Date:


Superintendent, WCBDD


Date


Board President, WCBDD


Date

The following definitions will apply:

FERPA – The Family Educational Rights and Privacy Act, which are federal regulations that govern the privacy of records maintained by schools, as well as the rights of parents and students to access those records. These regulations are codified in CFR Title 34 Part 99.

HIPAA – The Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320-1320d-9 and at 42 CFR Parts 160, 162 and 164. In common terms, this includes the HIPAA Enforcement Rule, Transactions Rule, Privacy Rule, Breach Notification Rule and Security Rule.

Information System – An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Security or Security Measures – Encompass all of the administrative, physical, and technical safeguards in an information system.

SECURITY MANAGEMENT PROCESS

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

1. The Superintendent will designate a HIPAA Security Officer. The job responsibilities for this individual are detailed in the Attachment: Sample Privacy & Security Officer Job Descriptions. The HIPAA Security Officer will assume the duties detailed in OAC § 5123:2-1-02(1)(&)(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 01-ALL-ALL-0139 HIPAA Privacy and Procedure 02-ALL-ALL-0656 (AD) Maintenance of HIPAA Required Documentation.
2. The HIPAA Security Officer will be responsible for security management process. This will include:
 - A. **Security Team.** The HIPAA 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:
 - a. The county board will use the risk assessment methodology detailed in NIST SP 800-30 (July 2002)
 - b. The results of this assessment shall be documented and maintained for 6 years
 - c. 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
 - a. Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices.
 - b. 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.
 - c. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level so as to comply with HIPAA regulations.
 - d. Train board staff regarding compliance
 - e. Monitor board compliance with the information security policies, and take action as appropriate based on this monitoring
 - D. **Information System Inventory.** The HIPAA Security Officer and/or Security Team shall maintain an inventory of the hardware, software, and networking infrastructure.
 - a. Content of Inventory:
 - i. 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.
 - ii. Network infrastructure documentation will include network topology and all other information necessary to recreate the network in the event of a catastrophic event
 - iii. Software inventory will include hardware installed on, Software manufacturer, program name, version number, license/serial number and date.
 - b. Update frequency. This inventory should be updated on an ongoing basis with a physical inventory no less frequent than

annually for mobile devices.

- c. **Network Monitoring.** Network access monitoring will be performed to validate that devices which access the network are all included in the inventory. Corrective action will be taken when an unknown device appears.
- d. **Backup copy.** A copy of this inventory shall be maintained off-site to insure availability in the event of a fire or other disaster.

DATA BACKUP

The HIPAA Security Officer will insure that a robust data backup regimen is in place and operational at all times. They shall personally insure that the procedures below are consistently maintained.

1. **Data Criticality Analysis.** A Data Criticality Analysis shall be performed and updated as appropriate. The backup regimen must be developed in a manner consistent with the data criticality.
2. **Multiple Backup Generations.** Backups should include as many generations as is practical to store. One backup per day is appropriate.
3. **Backup Software.** Appropriate backup software shall be maintained, with appropriate scripting. These scripts shall be reviewed and adjusted as appropriate whenever hardware or software upgrades are performed to insure that appropriate data backup is maintained.
4. **Off-Site Storage.** Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include an off-site backup, that is, in a separate facility from the one containing the physical hardware.
5. **Backup Documentation.**
 - A. A written description of the backup regimen must be maintained, including a description of the backup software utilized, the backup method used (e.g. full system or incremental), details of the generations maintained, naming conventions used, names of backup scripts, and other information necessary to understand the backup strategy.
 - B. User documentation, for use by a system administrator, shall be maintained to allow for an alternate person to verify the daily operation of the backup.
6. **Responsibility.** The HIPAA Security Officer shall designate the employee with primary responsibility personally handle the backup. In the event that he/she is absent from work, an alternate individual shall be responsible. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
7. **Backup Log.** A daily written log shall be maintained documenting the date, person, verification that backup was completed successfully, and any comments. Problems should be immediately reported to the HIPAA Security Officer, or if the HIPAA Security Officer is away from the office, to the Superintendent.
8. **Backup Media Security.** Backup media shall be maintained in a secure location.
9. **Testing and Plan Revision.** REVIEW AND UPDATE OF THE DATA BACKUP PLAN SHOULD BE CONDUCTED WITH ANY SIGNIFICANT UPDATE OF THE TECHNICAL ENVIRONMENT. On at least a quarterly basis, a trial restore shall be performed from the backup to verify the proper function of the backup process. Based on the results of this test, and any other environmental changes, the Data Backup Policy and Disaster Recovery Plan shall be updated. The results of this process should be documented and maintained for 1 year.
10. **Data Recovery Plan.** The HIPAA Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

DISASTER RECOVERY PLAN AND EMERGENCY MODE OPERATION

Board personnel shall develop contingency plans to prepare for system failures, and for procedures for maintaining critical board operations in the event of system failure.

1. **Disaster Recovery Team.** If appropriate, the HIPAA Security Officer shall establish a Disaster Recovery Team to assist in the preparation of contingency plans as well as to execute assigned tasks in the event of a disaster. The HIPAA Security Officer shall direct this team and is responsible for all tasks identified in this policy.
2. **Scenario Identification.** Contingency planning shall begin with identification of likely failure scenarios. These scenarios should include, at a minimum, failure of one or more servers, data corruption of one or more subsystems, and catastrophic loss of the entire facility due to fire or other natural disaster. These scenarios shall be included in the written plan, and serve as the basis for the measures outlined below.
3. **Preventative Measures.** The HIPAA Security Officer shall, on an ongoing basis, evaluate the activities that are critical to board operations and implement preventative measures to reduce the likelihood of system failure. These would include technical measures such as RAID arrays, backup power supplies, fire suppression systems, raised floors, security systems, database transaction logging and the like.
4. **System and Data Recovery Plan.** The HIPAA Security Officer shall maintain a written system and data recovery plan, and take reasonable steps to mitigate losses, for likely failure scenarios. The written plan should include:
 - A. Computer applications shall be reviewed and assessed as to their criticality for maintaining board operations. The results of this assessment shall be documented.
 - B. Development of written documentation of tasks and responsibilities for members of the Disaster Recovery Team in the event of various failure scenarios.
 - C. System configuration documentation, as specified in the policy "HIPAA Security Officer and Security Management Process" to facilitate replacement of vital equipment in the event of a catastrophic loss.
 - D. Complete and current employee information and vital records.

- E. Identification of, and contact information for, vendors who will be used for replacing equipment following a disaster. Reasonable steps to assure rapid recovery and mitigate losses can include, if appropriate:
 - A. Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by board management.
 - B. Contracts with hot and/or cold system sites if deemed necessary and prudent by board management
 - C. Steps to manage risk, such as insurance policies, as deemed appropriate, for possible losses to mitigate the financial impact of disasters.
- 5. **Emergency Mode Operations Plan.** The HIPAA Security Officer shall maintain a plan to maintain vital operations in the event of a partial or complete system failure. This should begin with an identification of likely failure scenarios as described above. Elements of this plan may include:
 - A. Identification of situations which occur where immediate access to individual data is necessary, as in certain MUI's involving health emergencies.
 - B. Maintenance of Critical Individual Data from electronics in a paper chart, or other plan to protect against loss of access due to technical failure.
 - C. People assigned to assist Case Managers or other individuals with immediate access to this information in the event of an emergency regarding an individual (accident, medical incident, etc.)
 - D. Periodic training of staff, regarding how to access information in the event of simultaneous computer downtime and individual emergency.
 - E. For non-emergency situations, procedures which allow staff to function, to the extent possible, in the event of system downtime.
- 6. **Plan Testing.** The HIPAA Security Officer shall be responsible for plan testing. He or she shall design the approach to testing and the level of resources which are appropriate to invest in these activities based on the risk analysis.
- 7. **Off Site Storage of Key Documents.** A copy of the key documents described in this policy shall be maintained off site, in either paper or electronic form, so that they are readily and quickly assessable in the event of catastrophic loss of the facility.

Attachment: Sample Privacy & Security Officer Job Descriptions

References: 34 CFR Part 99
 45 CFR Part 164; 164.308(a)(7); 164.312(a)(1)
 42 USC §§ 1320-1320d-8
 Center for Internet Security at www.cisecurity.org
 CERT at www.cert.org
 NIST SP 800-14
 NIST SP 800-18
 NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, 2001
 NIST SP 800-30, Risk Management Guide for Information Technology Systems, 2001
 NIST SP 800-53
 OAC § 5123:2-1-02(I) & (I)(7) & (A)(5)
 SANS at www.sans.org
 01-ALL-ALL-0139
 02-ALL-ALL-0656 (AD)

mms\policy\0161

SAMPLE PRIVACY & SECURITY OFFICE JOB DESCRIPTIONS

HIPAA PRIVACY OFFICER JOB DESCRIPTION

The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the WCBDD's policies and procedures covering the privacy of, and access to, individual health information in compliance with federal and state laws and the WCBDD's information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of WCBDD information privacy policies and procedures in coordination with WCBDD management and administration, the HIPAA Committee, and legal counsel.
- Works with WCBDD senior management to establish an WCBDD-wide HIPAA Committee.
- Serves in a leadership role for all HIPAA activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works with legal counsel and the HIPAA committee to ensure the WCBDD has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current WCBDD and legal practices and requirements.
- Oversees, directs, delivers, or ensures delivery of privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
- Participates in the development, implementation, and ongoing compliance monitoring of all business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Assists HIPAA Security Officer with handling of any security incidents and/or security rule violations.
- Establishes with management and operations a mechanism to track access to protected health information, within the purview of the WCBDD and as required by law and to allow qualified individuals to review or receive a report on such activity.
- Works cooperatively with the applicable WCBDD units in overseeing individual rights to inspect, amend, and restrict access to protected health information when appropriate.
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the WCBDD's privacy policies and procedures and, when necessary, legal counsel.
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the WCBDD's workforce, extended workforce, and for all business associates, in cooperation with administration, and legal counsel as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the WCBDD and related entities.
- Assists HIPAA Security officer by reviewing all system-related information security plans throughout the WCBDD's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Works with all WCBDD personnel involved with any aspect of release of protected health information, to ensure full coordination and cooperation under the WCBDD's policies and procedures and legal requirements
- Maintains current knowledge of federal privacy laws, specifically HIPAA and FERPA, as well as state privacy laws, accreditation standards, and monitors advancements in information privacy technologies to ensure WCBDD adaptation and compliance.
- Serves as information privacy consultant to the WCBDD for all departments and appropriate entities.
- Cooperates with the Office of Civil Rights and other legal entities in any compliance reviews or investigations.
- Works with WCBDD administration, legal counsel, and other related parties to represent the WCBDD's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

Qualifications of Privacy Officer:

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of health information management, project management, and change management.
- Demonstrated organization, facilitation, communication, and presentation skills.

SAMPLE PRIVACY & SECURITY OFFICE JOB DESCRIPTIONS

HIPAA SECURITY OFFICER JOB DESCRIPTION

The information security manager serves as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of individuals served, provider, employee and business information in compliance with organization policies, procedures and standards.

DUTIES:

- Reports to the Superintendent
- Document security policies and procedures created by the information security committee/council
- Provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures
- Initiate activities to create information security awareness within the organization
- Perform information security risk assessments and act as an internal auditor
- Serve as the security liaison to clinical administrative and behavioral systems as they integrate with their data users
- Implement information security policies and procedures
- Review all system-related security planning throughout the network and act as liaison to information systems
- Monitor compliance with information security policies and procedures, referring problems to the appropriate department director
- Coordinate the activities of the information security committee
- Advise the organization with current information about information security technologies and issues
- Monitor the access control systems to assure appropriate access levels are maintained
- Prepare disaster prevention and recovery plan

QUALIFICATIONS:

- Information security certification, such as the CISSP, is preferred