# POLICY 2500

## COMPUTER SECURITY

*HIPAA, FERPA, IDEA and Ohio Revised Code Compliance*

## Table of Contents

# 2500 HIPAA SECURITY POLICIES

# 2500.01 POLICIES FOR EXECUTIVE MANAGEMENT & HIPAA SECURITY OFFICER

## *2500.01.01 Security Management Process*

**POLICY**
CCBDD will appoint a HIPAA Security Officer. The HIPAA Security Officer will orchestrate the Agency's security management process.

**AUDIENCE**
Executive Management

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(2)

**PROCEDURES**
1) **The Superintendent will designate a HIPAA Security Officer**. The job responsibilities for this person are detailed in Appendix A – Sample Job Descriptions for HIPAA Privacy Officer and Security Officer. Documentation of the designation of the HIPAA Security Officer will be retained with other HIPAA-mandated designations per Policy 2400.03 HIPAA Assignments and 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 Agency. The Security Team's charter would be defined by the Agency, 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 Analysis**. A risk analysis will be conducted and updated periodically. The Risk Analysis is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information maintained on systems owned or used by CCBDD. The Computer Security Risk Analysis will be handled as follows:
      a) CCBDD will use the risk analysis methodology detailed in NIST SP 800-30 Revision 1.
      b) The results of this analysis shall be documented and maintained for 6 years
      c) The risk analysis shall be updated on an annual basis, or more frequently if appropriate based on technical and environmental variables, major software updates, infrastructure or other technological changes.
      d) The risk analysis shall be reviewed by the Security Officer, Privacy Officer, Superintendent, and any other person(s) involved in risk management decision making or implementation. CCBDD will maintain written documentation that these persons reviewed this risk analysis, and will maintain that documentation for 6 years.
   C) **Risk Management**. CCBDD shall manage the risks identified in the risk analysis:
      a) CCBDD's Superintendent, in conjunction with the Board of Trustees, shall articulate a risk threshold, that is, a dollar amount of risk that the organization is willing to accept.
      b) Risks greater than this threshold should be either mitigated, that is the probability should be reduced, or transferred, either through contract or insurance. These decisions may be made by the Superintendent or his/her designee.

      The results of risk management decisions, and corrective action taken, including the timeframe for corrective action, shall be documented. Documentation shall be maintained for 6 years.
   D) **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 of Trustees as necessary, including implementation of new and updated policies, acquisition of technical security measures, or physical security measures.
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 Agency staff regarding compliance.
v) Monitor Agency compliance with the information security policies, and take action as appropriate based on this monitoring.

E) **Information System Inventory**. The HIPAA Security Officer and/or Security Team shall maintain an inventory of the hardware 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.
i) Update frequency. This inventory should be updated on an ongoing basis with a physical inventory no less frequent than annually for mobile devices.
ii) 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.
iii) Backup copy. A copy of this inventory shall be maintained at a separate location to ensure availability in the event of a fire or other disaster.

**E) Change Management.** The HIPAA Security Officer shall proceed prudently with any changes to hardware or software.
i) A full backup of any major software system will be performed prior to any software upgrade or movement of a server, to allow for restoration of a working copy in the event of malfunction. After upgrade, key functionality of system will be promptly verified so that the practice can revert to the previous version if necessary.
ii) Prior to patching operating system or DBMS software on a server, the application software vendor will be contacted for validation that functionality has been tested and that no compatibility issues have been found. Automatic patching shall not be enabled on servers.
iii) Interfaces will be monitored upon change of a software application on either end to validate proper functionality.

**REFERENCES**

*NIST SP 800-30 Rev 1, Risk Management Guide for Information Technology Systems*

Center for Internet Security at www.cisecurity.org

# *2500.01.02 Data Backup*

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

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR §164
45 CFR §164.308(a)(7)

**PROCEDURES**
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 ensure 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 to personally handle the backup. In the event that he/she is absent from work, an alternate person shall be responsible. All persons responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
7) **Backup Media Security**. Backup media shall be maintained in a secure location.
8) **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.
9) **Data Recovery Plan.** The HIPAA Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

# *2500.01.03 Disaster Recovery Plan and Emergency Mode Operation*

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

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR §164
45 CFR §164.308(a)(7)
45 CFR §164.312(a)(1)

**PROCEDURES**
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 Agency 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 Agency 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 Agency management.
   B) Contracts with hot and/or cold system sites if deemed necessary and prudent by Agency 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 MUIs involving health emergencies,
   B) Maintenance of Critical Individual Data from electronic 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 persons 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 accessible in the event of catastrophic loss of the facility.

**REFERENCES**

NIST SP 800-14
NIST SP 800-18
NIST SP 800-26
NIST SP 800-30
NIST SP 800-53

# *2500.01.04 Facility Security and Access Control*

**POLICY**
All employees shall be aware of facility security and access policies to ensure that only authorized personnel have physical access to the facility and its equipment.

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(a)(1)

**PROCEDURES**
1) **Facility Security Planning**. The HIPAA Security Officer shall periodically evaluate physical security vulnerabilities, identify corrective measures, and develop a written facility security plan. The plan should focus especially on security of:
   A) Computer Servers
   B) Telephone and Networking equipment
   C) IT staff offices
   D) Workstation locations
   Attention should be given to areas with public access, whether workstations are protected from public access or viewing, the security of entrances and exits, and normal physical protections (locks on doors, windows, etc.).
2) **Employee Training**. The HIPAA Security Officer shall be responsible for employee training on their duties and responsibilities for facility security as described in the facility security plan.
3) **Maintenance of Physical Security Equipment**. The Director of Operations shall be responsible for maintaining equipment necessary to secure the facility, including locks, alarm systems, doors, security lighting, etc. Records of repairs and modifications shall be maintained.
4) **Unauthorized Persons**. Any staff who sees an unauthorized, unescorted person in the facility, except for those Public Access Areas, shall, in a polite manner, escort the person to a common area. Any suspicious incident shall be reported to the HIPAA Security Officer and/or police.

**REFERENCES**

NIST SP 800-66

# *2500.01.05 Annual Security Evaluation*

**POLICY**
Annually the HIPAA Security Officer shall conduct a technical evaluation of the Agency's security policies and procedures, including a revised risk assessment, and update policies as necessary in response to environmental or operational changes affecting the security of electronic protected health information.

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(8)

**PROCEDURES**
1) **Annual Review of Regulations, Statutes, and Technological Issues to Update Security Policies.** On an annual basis, the HIPAA Security Officer will review any updates to federal HIPAA regulations, other applicable federal and/or state statues, and technological issues and update the organization's security policies as appropriate. This review may be conducted internally, or upon the HIPAA Security Officer's recommendation and approval by the superintendent and/or Board of Trustees, contracted to an outside firm.
2) **Annual Evaluation.** On at least an annual basis, an evaluation of the technical infrastructure and/or the organizations compliance with computer security regulations will be conducted. From year to year, type of evaluation(s) may vary and will be selected by the HIPAA Security Officer. Appropriate evaluations may include
   A) Vulnerability scanning and remediation
      a) a commercial or open-source vulnerability scanning tool is used and/or a service is employed
      b) Vulnerability scanning is performed both from outside of the network (targeting public facing IP addresses) and from inside the network
      c) Devices connected to the devices are compared to the IT Asset inventory to identify unknown devices connected to the network
      d) Missing assets are identified
      e) Vulnerabilities shall be prioritized for remediation

      Remediation shall be performed in a prioritized basis
   B) Penetration tests
   C) Social Engineering exercises/tests
   D) IT Asset audits to identify missing assets
   E) Audits of policies and procedures for compliance with the following standards/regulations
      a) HIPAA
      b) CARF
      c) FERPA/IDEA
      d) State laws
   F) Audits of compliance with policies and procedures, including verification that the processes, procedures and documentation specified in the policies exist, and that the responsible personnel understand the policies

   Evaluations may be done more frequently, if determined by the Security Officer. More frequent evaluations are appropriate upon introduction of new technologies, the emergence of new environmental risks, regulatory changes, change in personnel, or other factors. Evaluations may be targeted to a specific area.
3) **Report and Recommendations.** The HIPAA Security Officer shall submit their report to the Superintendent and/or Board of Trustees, including any recommendations.
4) **Documentation of Review.** The results of the review will be documented, and documentation shall be retained for 6 years.

# *2500.01.06 Audit Control and Activity Review*

**POLICY**
System capabilities for maintaining audit trails of system use shall be enabled to permit forensic analysis and periodic activity reviews. Periodic activity reviews should be conducted to identify inappropriate activity so that appropriate corrective action is possible.

**AUDIENCE**
HIPAA Security Officer
HIPAA Privacy Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(b)
45 CFR § 164.308(a)(1)
45 CFR § 164.308(a)(5) Log-in Monitoring

**PROCEDURES**
1) **System Activity Logs**. Activity logs shall be enabled at the following levels:
   A) **Operating System**: Audit Policy should be set to log logon events, account management events, policy changes, and system events.
   B) **Firewall Hardware and Software**: Logs should be enabled to track inbound and outbound activity, including internet access by person.
   C) **Application Software Logging**: All software which stores data on Individuals served shall have audit trail capabilities. Logs should be enabled in application software such as clinical record software, billing software, or information systems which store information regarding Individuals being served.
2) **Security on Logs**. Appropriate security features and passwords should be used at all levels above to permit log file access only by the HIPAA Security Officer and/or a person designated by him/her.
3) **Annual Audit of PHI Access**. A review of system activity will be conducted on at least a quarterly basis. The HIPAA Privacy Officer shall design an audit strategy to identify probable or anticipated violations. Suspicious and/or inappropriate activities include but are not limited to:
   A) Access by persons at unusual hours.
   B) Higher access/usage levels than normal.
   C) Accesses to records of relatives of celebrities, celebrities' children or employees.
   D) Unauthorized changes to security settings.
   E) Web sites viewed by employees to verify that they are work related.
   F) Outside probe attempts and/or accesses via the internet connection.
   G) Other Unusual patterns of activity.
4) **System Activity Review**. In a manner determined by the HIPAA Security Officer, he or she will monitor system activity to detect suspicious or unusual system activity.
5) **Corrective Action.** The HIPAA Security Officer will initiate corrective action, in conjunction with other members of the management staff, in the event any inappropriate PHI access, or if suspicious or unusual system activity is detected.
6) **Purge of Log files**. System Log files which grow large may be purged under the direction of the HIPAA Security Officer.
7) **Annual Policy Review**. Annual attention should be given this policy regarding audit controls, as the threat level varies and the cost of monitoring tools changes.

# *2500.01.07 Malicious Software Protection*

**POLICY**
All company computer systems will be protected by virus and malicious software protection capabilities.

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5)

**PROCEDURES**
1) **Multi-Layered Defense Strategy.** The HIPAA Security Officer will ensure that the computer network be protected from malicious software using a multi-layered defense strategy:
   A) Appropriately configured, commercial-grade firewall (per Policy 2500.01.11 Technical Safeguards)
   B) Centrally managed and updated anti-virus software
   C) DNS filtering service to limit connections to malicious sites, phishing attacks, and botnets per Policy 2500.01.11 Technical Safeguards
   D) Patching of operating system and application software per Policy 2500.01.11 Technical Safeguards
   E) Monitoring system logs per Policy 2500.01.06 Audit Control and Activity Log Review
2) **Special procedures** will be used, if appropriate, for any users who routinely access on-line banking accounts.
3) **Annual Review.** Annual review of this policy will be conducted to ensure that the products, services, and configuration, and policies appropriately manage risk for this rapidly evolving threat.

# *2500.01.08 Breach Reporting*

**POLICY**
The Agency will notify Individuals receiving services, the Secretary of HHS and, when appropriate, the news media regarding breaches of protected health information.

**AUDIENCE**
HIPAA Security Officer, HIPAA Privacy Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164, Subpart D
45 CFR § 164.400, 45 CFR § 164.402, 45 CFR § 164.404, 45 CFR § 164.406, 45 CFR § 164.408, 45 CFR § 164.410, 45 CFR § 164.412, 45 CFR § 164.414

**PROCEDURES**
1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Security Officer and HIPAA Privacy Officer shall jointly determine if the incident meets the definition of a breach. If a Security Incident Response Team (Team) has not been assembled, they may assemble a Team at this point. Legal counsel and other outside expert advice shall be obtained, if appropriate, for additional guidance on the Team. An investigation should be launched, with attention to preserving evidence. The Team shall follow the following 3 step procedure:
   A) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   B) Does one of the statutory exceptions listed in the breach definition in Policy 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   C) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      iii) Whether the protected health information was actually acquired or viewed; and
      iv) The extent to which the risk to the protected health information has been mitigated.

   The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 2400.03.03 HIPAA Assignments and Documentation. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred and this process may stop. Otherwise, a breach has occurred and the Team should proceed with the steps that follow in the remainder of this policy.
2) **Public Relations Strategy**. The Team should develop a public relations strategy to include when and who should speak to the media and what should be said.
3) **Breach Notification**. In the event of a breach, the Team shall:
   A) Notify Individuals affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      i) In the event of an urgent situation, the Agency may use telephone, email or other means to immediately notify Individuals of the breach.
      ii) Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following:
         1) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
         2) A description of the types of unsecured protected health information that were involved in the breach;
         3) Any steps that Individuals should take to protect themselves from potential harm resulting from the breach;
         4) A brief description of what the Agency is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and
         5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site or postal address.

iii) Send the primary breach notification to:
1) Individuals affected by the breach by first-class mail at their last known address, or by e-mail if agreed in advance by the Individual for this type of notice, or
2) Parent, guardian, or HIPAA Personal Representative of the Individual in the event the Individual is a minor and/or not competent to make decisions, or
3) next of kin or personal representative of the Individual in the event that the Individual is deceased and the next of kin name and address are available.

iv) Track returned mail and provide a substitute notice to Individuals who did not receive the primary notification (no further effort is necessary for unreachable next-of kin):
1) In the event that fewer than 10 Individuals, the HIPAA Privacy Officer shall research updated address and/or phone number and make best efforts to inform those Individuals by either phone or mail.
2) In the event that 10 or more Individuals are not reachable by first class mail,
a) A toll-free phone number shall be established, and staffed with operators, for at least 90 days
b) a notice shall be conspicuously placed on the Agency's web site home page with details of the above details on the breach plus the phone number

B) Notify the news media if more 500 Individual records are involved in the breach
i) Under direction of the Agency superintendent, a press release shall be prepared detailing the information in section 3Aii above, and other relevant information.
ii) Upon approval of the Superintendent, the press release shall be issued without unreasonable delay (and in no case later than 60 days after discovery of the breach) to the major print, broadcast and online media serving the county.

C) Notify the Secretary of the Department of HHS regarding the breach
i) In the event that the breach involves 500 or more Individuals, notice to the Secretary should be provided at the same time as the Individual notification in the manner detailed on the HHS Web site.
ii) For breaches involving fewer than 500 Individuals, a log including at a minimum the information in 3Aii above, and other relevant information, should be maintained. At the end of the calendar year, the contents of the annual log should be provided to the secretary in the manner detailed on the HHS Web site.

2) **Breaches by Business Associates**. Breaches by business associates are handled in the same manner. Business associates are obligated to cooperate in providing necessary information; the Agency is responsible for issuing the notice detailed in this policy.

3) **Law Enforcement Delay**. The notices to Individuals and the media may be delayed if a request is received by a law enforcement official:
A) If written notice is received from a law enforcement official which specifies the time period of delay, the Agency shall comply with that request.
B) If the request is made orally, the notification shall be delayed but not longer than 30 days from the date of the oral request.

4) **Documentation**. Documentation, including any notices provided, incident reports, meeting notes, especially those which document the date of the breach, shall be maintained for 6 years. For the legal purposes, including the timelines in policy, the date of breach discovery shall be the date that the Agency should have become aware if it exercised reasonable diligence.

# *2500.01.09 Security Awareness Program*

**POLICY**
The HIPAA Security Officer will conduct an ongoing security awareness program to train and refresh staff on computer security behaviors and the Agency's security policies. Priority topics shall include recognizing and avoiding malicious software, avoiding "social engineering" ploys, using passwords effectively, and adhering to workstation use policies.

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5)

**PROCEDURES**
1) **Security Training Program for New Employees.** The HIPAA Security Officer shall develop, and maintain, a security training program for new employees. This should include, at a minimum:
   A) Password policies
   B) Recognizing and avoiding malicious software
   C) Understanding e-mail attachments
   D) Safe web browsing practices
   E) Dangers of downloading files from the internet
   F) Understanding of "Social Engineering" and how to recognize such ploys
   G) Knowledge of Workstation Use Policies
   H) Consequences for non-compliance
   I) Security Incident Reporting Procedures

   Other appropriate topics may be included at the discretion of the HIPAA Security Officer. The program may be conducted one-on-one, via e-learning system, or other media as determined by the HIPAA Security Officer.
2) **Upon initial implementation**, the Security Training program will be provided to all staff. Subsequently, all new staff should receive the training.
3) **Periodic security awareness training will be provided to all employees**. The HIPAA Security Officer shall develop an annual plan specifying the scope of the program; the goals; the target audiences; the learning objectives; the deployment methods; evaluation and measurement techniques; and the frequency of training. Possible topics would include:
   A) Reinforcement of topics for the Security Training Program and Security Policies
   B) Advisories regarding current threats
   C) Issues with new technologies such as smartphone/tablet security

   A variety of media and avenues should be explored such as sign-in banners, security reminder cards for posting at workstations, articles in employee newsletters, posting on bulletin boards, etc. At a minimum, Computer Security Awareness will be included annually as detailed in Policy 320 Orientation and Training.

# *2500.01.10 Device and Media Disposal and Re-Use*

**POLICY**
Electronic storage media and devices shall be cleaned of protected health information and other confidential information prior to disposal and/or re-use.

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(d)(1)

**PROCEDURES**
1) **Media Disposal Handled by HIPAA Security Officer**. As specified in Policy 2500.04.01 Computer Usage, Agency employees are prohibited from storing Protected Health Information of the Agency's on removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee should be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed.
2) **Technical Guidance**. In accordance with instructions from the Secretary of HHS, technical guidance regarding media disposal should be obtained from NIST SP 800-88 *Guidelines for Media Sanitization*. The Agency requires that at a minimum, data from electronic media should be "cleared", as defined in the referenced NIST documentation.
3) **Media Disposal and Re-use**. Procedures vary based on type of storage media:
   A) **CDs, DVDs and Tapes**: CDs, DVDs and Tapes should be physically destroyed by a service who will issue a certificate of destruction.
   B) **Hard Drives**. Hard drives and floppy disks shall be physically destroyed.
   C) **Other Media**. See NIST SP 800-88 for disposal/recycling methods for other media.
4) **Records.** Records of Media disposal should be maintained for 6 years. The following records should be maintained:
   A) Item Description
   B) Make/Model
   C) Serial number(s) / Property Number(s)
   D) Backup Made of Information (Yes/No)
   E) If Yes, location of backup
   F) Item Disposition (Clear/Purge/Destroy)
      i) Date Conducted
      ii) Conducted by
      iii) Phone #
      iv) Validated By
      v) Phone #
   G) Sanitization Method used
   H) Final disposition of media (Disposed/Reused Internally/Reused Externally/Returned to Manufacturer /Other)

# *2500.01.11 Technical Safeguards*

**POLICY**
Technical Safeguards will be employed as necessary to maintain the integrity of data, and to ensure the security of data during transmission.

**AUDIENCE**
HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(c)
45 CFR § 164.312(d)
45 CFR § 164.312(e)

**PROCEDURES**
1) **Firewalls.** Commercial-grade hardware and/or software firewalls shall be employed to protect against network intrusions and to manage/monitor outbound traffic. Workstation-based software firewalls (e.g. Windows Firewall) should be used on laptop computers since they may be connected to an outside network.
2) **Secure Configurations.** Workstations and servers will be installed with a standard configuration that meets the following specifications:
   A) A standard list of software to be installed will be maintained. Only vendor-supported versions of software should be used. Additional software may be installed for specific users based on unique requirements.
   B) Windows, Microsoft Office, and Internet Explorer should be securely configured. Microsoft's security configuration guides shall be used, using the middle level of security, with modifications as necessary to allow for functionality.
   C) Microsoft Security Compliance Manager and Active Directory will be used to maintain and enforce security configurations.
3) **Operating System and Application Software Patching**. Operating Systems, application software and hypervisors, if used, shall be patched regularly on both servers and workstations. Auto-update functionally may be employed and update servers. Centralized patch management software such as Microsoft WSUS and/or third party-software may be utilized.
4) **Virtualization Software and Environment**. If virtualization technology is employed, the virtualization-enabling software, aka "hypervisors", shall be secured as follows:
   A) Unneeded capabilities shall be disabled to reduce potential attack vectors.
   B) A strong password (minimum of 8 characters, 1 upper case, 1 lower case, 1 digit) shall be used for the management console.
   C) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's.
   D) Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations.
5) **DNS Filtering** shall be employed to reduce access to unsafe websites and to reduce phishing attacks, using OpenDNS or an alternative service.
6) **Wireless Networks**. Wireless networks, if employed, will be implemented with the following security options:
   A) The beacon shall be enabled.
   B) The SSID should be changed from the default.
   C) WPA/WPA2 should be enabled.
   D) WPS should be disabled.
   These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
7) **E-mail**. For transmission of PHI, secure, encrypted e-mail should be employed.

8) **Encryption of desktop, mobile devices and portable media**. When encryption of end-user devices is determined appropriate based on risk analysis, the Agency shall employ the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically, the Agency should:

A) consider solutions that use existing system features (such as operating system features) and infrastructure;
B) use centralized management for all deployments of storage encryption except for standalone deployments; and very small-scale deployments;
C) select appropriate user authenticators for storage encryption solutions; and
D) implement measures that support and complement storage encryption implementations for end user devices.

9) **Transmission Security**. For data in motion, the HIPAA Security Officer implement solutions consistent with the Secretary of HHS's guidance on securing PHI. Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in:
   A) NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*.
   B) NIST 800-77, *Guide to IPsec VPNs*.
   C) NIST 800-113, *Guide to SSL VPNs*.
   D) Other FIPS 140-2 validated processes.
10) **Appropriate Audit Controls in Agency-Used Software**. Software used by Agency should be evaluated for the appropriate level of audit control, such as logging of all transactions or logging of key events such as creating, viewing, changing, or deleting PHI. In the event of deficiency of software currently in use, requests to vendors for enhancements should be made as appropriate. Appropriate audit controls should be a criterion for continued use of and/or procurement of any new operating or application software.
11) **Software utilizing Electronic Signatures**. The HIPAA Security Officer will review and approve any software that offers electronic signature capability prior to implementation at the Agency. The HIPAA Security Officer shall be responsible for implementation and ongoing monitoring/auditing of the software as specified in Policy 2500.01.13 Electronic Signatures.
12) **Automatic Log Off**. Appropriate measures shall be taken, based on the technology available, to enable the automatic log-off provisions as determined by the risk assessment. See also Policy 2500.04.01 Computer Usage and Policy 2500.02.01 Employee System Access and Termination Procedures.
13) **Integrity Checks**. The HIPAA Security Officer shall attend to integrity of electronic data:
   A) Periodic DBMS maintenance as recommended by the software vendor shall be performed.
   B) Message digest integrity reports shall be reviewed with corrective action taken as necessary.

Monitoring any electronic interfaces, such as lab interfaces, to verify proper functionality.

## *2500.01.12 Mitigation*

**POLICY**
In the event of an inappropriate use or disclosure of an Individual's PHI, the CCBDD will take reasonable steps to mitigate the harmful effects of the disclosure.

**AUDIENCE**
Privacy Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.530(f) – Mitigation

**PROCEDURES**
1) **Mitigating Harmful Effects of Privacy Violation.** In the event of a HIPAA Privacy rule violation, the Privacy Officer, in conjunction with other members of the management staff as he/she deems appropriate, shall take action to mitigate the harmful effects of the Privacy Violation, if this is reasonable and possible. The mitigation action should correspond to the nature of the violation. For example, if social security numbers are breached, it may be appropriate to purchase identity theft protection for 1 year.

# *2500.01.13 Electronic Signatures*

**POLICY**
Electronic signatures may be utilized at CCBDD by both employees and providers. Electronic signatures are legally binding as a means to identify the author and to confirm that the contents are what the author intended.

**AUDIENCE**
Employees Using Electronic Signatures; Managers

**AUTHORITY**
ORC § 1306 Ohio Uniform Electronic Transactions Act
ORC § 304 Electronic Records and Signatures for Counties
ORC § 9.01 Official Records – Preserving and Maintaining
ORC § 117.111 State Audits shall review method, accuracy and effectiveness of electronic signature security procedures

**DEFINITIONS**
1) Electronic Signature, as defined by the Ohio Revised Code, means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
2) Electronic facsimile. A computer image, such as one maintained in an electronic document imaging system, of a conventionally signed document is not an electronic signature. Rather, the electronic facsimile is legally equivalent to the original, traditionally signed document.

**PROCEDURES**
**1) Security**
A) **Confidentiality statement**. Anyone authorized to utilize electronic signature will be required to sign a statement attesting that he or she is the only one who has access to his/her signature/ logon password, that the electronic signature will be legally binding and that passwords will not be shared and will be kept confidential.
B) **Passwords**. All users will have their own user ID and password. Passwords must conform to complexity guidelines detailed in Policy 2500.04.01 Computer Usage.
C) **Personal Identification Numbers (PIN)/ Secondary Passwords.** PIN numbers and/or secondary passwords may be assigned when possible for use with electronic signatures to allow for another level of security (this is optional and county specific). PIN numbers or secondary passwords are not viewable on any screen.
D) Vendors, outside agency or providers who have access to using an application requiring an electronic signature based upon the user's ID and password as described in this policy, shall use additional controls to ensure the security and integrity of each user's electronic signature:
i) Follow loss management procedures to electronically de-authorize lost, stolen, missing or otherwise compromised documents or devices that bear or generate identification code or password information and use suitable, rigorous controls to issue temporary or permanent replacements;
ii) Use safeguards to prevent the unauthorized use or attempted use of passwords and/or identification codes; and
iii) Test or use only tested devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered.

2) **Creating, Maintaining an Electronic Signature**
A) Electronic signatures can be used wherever handwritten signatures are used except where stated by a specific law or rule.
B) All who use a system that uses electronic signatures are required to review their entries.
C) Once an entry has been signed electronically, the computer system will prevent it from being deleted or altered. If errors are later found in the entry or if information must be added, this will be done by means of addendum to the original entry. The addendum should also be signed electronically and date/time stamped by the computer software.

D) System specific standards and procedures for use may vary by system and it will be required that the Agency must establish and maintain system specific procedures for any system which also satisfies other current policies.

3) **Auditing Electronic Signature Procedures**
The computer software and anyone using the software system must use a secure, computer-generated, time-stamped audit trail that records independently the date and time of user entries, including actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Audit trail documentation shall be retained for a period at least as long as that required for the record and shall be made available as needed upon request. Any misuse or disregard of electronic signature policy will be reviewed and acted upon by the Superintendent or designee.

4) **Review and Approval Prior to Using Electronic Signatures**
The HIPAA Security Officer shall review the software utilized for electronic signatures, and other procedures utilized, for compliance with this policy prior to permitting the use of electronic signatures. This review shall be conducted for each transaction to be electronically signed.

# 2500.02 SECURITY POLICIES FOR HR STAFF & SUPERVISORS

## *2500.02.01 Employee System Access and Termination Procedures*

**POLICY**
System access will be granted to employees in a manner consistent with the HIPAA Privacy laws and other state regulations, including specific policies for access control, granting access to new staff and staff with assignment changes, handling staff terminations, password selection, maintenance and use, and access to the system in the event of an emergency.

**AUDIENCE**
Human Resource Department, Supervisors, HIPAA Security Officer

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(3)
45 CFR § 164.308(a)(4)
45 CFR § 164.312(a)(1)
45 CFR § 164.314(d)
45 CFR § 164.308(a)(5) Password Management

**PROCEDURES**

**AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS**

**Audience: HIPAA Security Officer, Privacy Officer**

1) **Minimum Necessary Analysis.** The HIPAA Security Officer shall coordinate with the Privacy Officer to maintain and document a current "minimum necessary" analysis, per Policy 2400.01.03 Minimum Necessary Policy which identifies the classes of persons (job descriptions) and the categories of Protected Health Information which they need access to.
2) **Access Profiles.** The HIPAA Security Officer shall utilize the security capabilities of the various network and application software systems at the Agency and develop role-based "Access Profiles" for these different job descriptions. Vendors will be contacted for any enhancements necessary for appropriate implementation of these access profiles.
3) **Granting Access to Information Systems**. The authority to grant access to information systems rests with Superintendent and is delegated to the hiring manager. Implicit in a hiring decision is the provision of access to the information systems necessary for the job, as determined above based on the minimum necessary analysis and the Access Profiles.
4) **Granting Access Beyond the Standard Access Profile**. In certain situations, such as when employees are assigned special projects, information access may be required beyond what the job description would dictate. In these cases, the HIPAA Security Officer, after any necessary consultation with the management staff at the Agency, shall have the authority to grant access to information systems which go beyond the standard Access Profiles described above. Access should be terminated when the need for access is completed.
5) **Inventory of Employees with Access to PHI.** The HIPAA Security Officer shall maintain an updated, inventory of employees with access to PHI and the access rights which are granted.
6) **Annual Audit of Access Controls.** On an annual basis, the HIPAA Security Officer shall audit the access controls to verify that the above policies have been implemented properly and consistently. Such an audit could include verification that recently terminated employees no longer have access, a review of access for employees with job changes in the previous year, and a random sampling of other employee access authorization. Based on the results of this audit, the HIPAA Security Officer shall adjust policies and/or staff training as appropriate.

**SYSTEM AND FACILITY ACCESS FOR NEW HIRES**

**Audience: Supervisors, Human Resource Department**

1) **Requests for Access to Information Systems.** Supervisors and/or the human resources department shall direct requests for access to information systems to the HIPAA Security Officer or his/her designee. The HIPAA Security Officer shall verify with the human resources department in the event of any question regarding the accuracy of the job assignment.
2) **Assigning User ID and Password.** The HIPAA Security Officer will assign new hires requiring computer access a unique network User ID and password, and/or User IDs and passwords for other application systems. Security settings appropriate for the person will be assigned in accordance with this policy, as described above.
3) **Communicating User ID and Password.** The HIPAA Security Officer shall communicate the User IDs and passwords in a manner which does not compromise security by revealing the passwords to another person.
4) **Documentation of System Access Rights**. As described above, the HIPAA Security Officer will maintain documentation of system access rights.
5) **User Data Area.** The HIPAA Security Officer will configure a User Data Area on the Server to provide data storage space for the employee. All data is to be stored on the server and not on workstations.
6) **Security Awareness Training.** Employees will receive Security Awareness Training, in the manner chosen by the HIPAA Security Officer, in accordance with the Policy 2500.01.09 Security Awareness Program. In addition, new employees should receive a written copy of the Policy 2500.04.01 Computer Usage, and they will sign written acknowledgement that they understand and will adhere to all policies. This will be maintained in the employee personnel file.

**PASSWORDS and PASSWORD MANAGEMENT**

**Audience: HIPAA Security Officer**

1) **Password Complexity**. Network policies shall be established to enforce password complexity as follows: 8 character minimum, minimum of 1 upper case letter, 1 lower case letter and 1 digit.
2) **Lockout**. The system shall lock accounts after 5 unsuccessful attempts.
3) **Password Reuse**. The system shall maintain the previous 5 passwords and prohibit re-use of any of these recent passwords.
4) **Password Changes**. The HIPAA Security Officer shall implement a mechanism to ensure that all employees change their passwords at least every 6 months.

**EMPLOYEE JOB CHANGES**

**Audience: Human Resources Department, HIPAA Security Officer**

1) The Human Resource Department shall notify the HIPAA Security Officer of all job changes so that adjustments to system access can be made if necessary.

**EMPLOYEE TERMINATION**

**Audience: Supervisors, Human Resource Department, HIPAA Security Officer**

1) **Change Employee Password and Disable User ID.** On the last day of employment, employee passwords to the network and Application Software will be changed and/or their User IDs will be disabled.
2) **Documentation.** The HIPAA Security Officer shall document the disabling of system access.
3) **Security Precautions for Involuntary Terminations.** For involuntary terminations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the head of human resources who shall coordinate with the Information Security Manager so that appropriate precautions will be taken to ensure the integrity and security of confidential Agency information. This could include such measures as:
   A) Physically escorting the person off the premises after notifying him/her of the termination.
   B) Disabling system access as specified above on a timely basis.
   C) Requiring all staff in the former employee's workgroup to change passwords.
   D) Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the person and perceived threat.

**EMERGENCY SYSTEM ACCESS**

**Audience: Supervisors, HIPAA Security Officer**

In the event of an emergency, such as a MUI in which immediate access to PHI is required, a staff member who does not have appropriate system permission but requires access shall contact the HIPAA Security Officer (or another staff person in that department) who will provide the necessary access on an expedited basis.

# 2500.04 SECURITY POLICIES FOR ALL STAFF

## *2500.04.01 Computer Usage*

**POLICY**
Each staff member is responsible for understanding and following the policies regarding workstation use and security.

**AUDIENCE**
All Staff

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.310(b) Workstation Use
45 CFR § 164.310(c) Workstation Security
45 CFR § 164.308(a)(5) Log in Monitoring

**PROCEDURES**
**WORKSTATION USE**

1) **System is for Job Duties**. Computer workstations, including use of internal systems, e-mail and the internet, are for use by employees to conduct their job responsibilities. These responsibilities include matters related to the Individuals served: their treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access to DODD systems, regulatory and business affairs, facilitating payment by 3rd party payers, and other matters which are specifically job related.
2) **Personal Use of Computer Workstation, Including Internet Use**. Employees are expected to be productive and to perform their job duties during work hours. Limited use of computer workstations is allowed for personal use. "Limited use" is not easily defined so employees should contact their supervisors for clarification. In general, "limited use" means:
   A) Employees may use their workstations for personal purposes on their "own time", which means before or after the workday, or during their lunch hour.
   B) At other times, personal use should be limited to brief accesses such as quickly checking the weather forecast.
   C) Workstations must never be used for any activity that would be embarrassing to the Agency if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
      i) downloading or viewing pornographic, racist, profane or otherwise objectionable material
      ii) conducting conversations of a sexual nature of relating to an illicit affair
      iii) relating to any illegal activity
      iv) political activity
      v) operating a business

      If an employee has any questions about whether a personal use is allowed, he or she should obtain permission from his/her supervisor.
   D) Personal use of Social Media, such as Facebook, Twitter, LinkedIn and others is detailed separately.
   E) Employees are prohibited from staying logged in to social media, instant messaging sites/tools, and their personal email except during their own time.
3) **E-Mail Use**. Employees with Agency e-mail accounts should check e-mail daily. Agency E-mail accounts in general are to be used for Agency purposes only. E-mail should be written in professional manner and should be courteous and respectful. Other policies when using e-mail:
   A) Use of e-mail internally is acceptable for transmitting PHI. Be aware that e-mail to outside parties is not secure and must not be used Protected Health Information unless it is appropriately encrypted.
   B) When participating in internet discussion groups, employees in general should clarify that their comments are their own and do not necessarily represent the Agency.
   C) Employees should recognize that email are considered a public record and subject to disclosure to the general public as detailed in Policy 801 Section 1 Public Records.
   D) For personal matters, employees must use a personal account such as Gmail or Yahoo mail, on a personally-owned device

   i) In the event that any Agency e-mail is received on a personal account, the employee must forward the email to the employee's Agency account so that it is entered into the public record.
   ii) In the event that a personal email is received on a Agency account, redirect the discussion to a personal email account.
4) **Storage of PHI or Confidential material to Removable Media Prohibited**. Personnel may not copy to removable media, such as Flash drives, CDs, DVD or portable hard drives, any Agency confidential information or Protected Health Information on Agency computer system, except when specifically authorized by the HIPAA Security Officer for Agency purposes.
5) **All Usage is Logged**. THE AGENCY RESERVES THE RIGHT TO MONITOR ALL USAGE OF AGENCY WORKSTATIONS, THROUGH THE LOGGING AND STORAGE OF ALL ACTIVITY, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES BROWSED, AND OTHER ACTIVITY, INCLUDING ANY PERSONAL USE OF AGENCY COMPUTERS. All logs of employee activity are property of the Agency.
6) **Data Storage on Network Only**. All data must be stored on the network, not on a workstation hard drive. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the appropriate User Directory on the server. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions on how to access their User Directory on the server. DATA STORED ON WORKSTATION HARD DRIVES IS NOT BACKED UP, AND MIGHT BE DELETED WITHOUT NOTICE. ALL DATA STORED ON THE NETWORK IS BACKED UP!
7) **Duplication of copyrighted material prohibited**. No employee may duplicate copyrighted software or other media using Agency equipment.
8) **Agency approved hardware only**. Only Agency-approved and installed hardware may be utilized. No wireless networking equipment, smartphones, video cameras, or other hardware or software may be installed or used without permission of the systems department. (Employees may use Guest WiFi with their smartphones, for personal use only, with no explicit permission.)
9) **Electronic signatures**. Employees using software that includes Agency-approved electronic signature capabilities shall follow all procedures specified in Policy 2500.01.13 Electronic Signatures

**WORKSTATION SECURITY**

1) Except with specific approval of the HIPAA Security Officer, workstations must not be setup in a public access area.
2) All employees should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.
3) Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.
4) Employees should logoff or lock their screen when leaving their workstation area for a period of time.
5) Workstations should be configured with automatic logoff capability so that they will become inaccessible after 20 minutes of system inactivity. Employees must not install any software on their computer without authorization from the HIPAA Security Officer, and must not alter or reconfigure network settings, printers, logging software, audit controls, or security settings without permission of the systems staff.

**USER IDs and PASSWORDS**

1) Each employee is assigned a unique User ID and Password. Employees must only use their User ID to access Agency systems – and employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Consequently, passwords should be kept secure and confidential and not shared with anyone else. If an employee reveals a password, or if becomes known to someone else, that employee must change the password.
2) Passwords should be at least 8 characters long and include upper case letters, lower case letters and numbers. The characters should not spell a single word or a person's name. Users are encouraged to use a pass-phrase which is a minimum of four words strung together. The password should not be related to the person in any way, as in a birth date, spouse, pet name, or anything which can be easily guessed.
3) In general, passwords should be memorized and not written. Any written reminder should not be maintained in the vicinity of the workstation.
4) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

**EMERGENCY SYSTEM ACCESS**

1) In the event of an emergency where immediate access to system information is required but not immediately possible, employees should contact the HIPAA Security Officer, who has contingency plans to allow access to vital data in a wide variety of scenarios (system down, MUIs, Individual emergencies which mandate system access by personnel who otherwise are not permitted access.)

# *2500.04.02 Social Media Use*

**POLICY**
Social media has become a significant communication medium in our world. Agency guidelines for using these sites and applications require that confidentiality and privacy of Individuals being served is maintained.

**AUDIENCE**
All Staff

**DEFINITIONS**
**Social Media –** means websites or applications that enable linking with other people, sharing information, and communicating. Popular examples include Facebook, Twitter, Instagram, Snapchat, LinkedIn, and others.

**PROCEDURES**
1) **Agency Sponsored Use**.
   A) The Superintendent may approve the establishment of an Agency-sponsored Fan Page, Group or Account.
   B) Superintendent will provide guidelines for Agency-sponsored use of social media.
2) **Personal use of social media by employees**.
   i) **Employee Use During Work Hours**. During work hours, employees are expected to focus on work-related activities. Consequently, in general, they are expected not to open any social media to avoid distraction and/or loss of employee productivity.
   ii) **Employee Use Outside of Work Hours**. Any statement or image on social media has the potential to become a public communication, so employees of the Agency must follow the following guidelines:
      1) **Sharing of work-related activities**. Employees should limit the sharing of any Agency-related information to information that they would deem acceptable to be made public, for example, on the front page of a major newspaper.
         a) Examples of information that are appropriate to share on social media include:
            i) The employee's excitement and satisfaction with the work and mission of the Agency.
            ii) Details of an upcoming public event sponsored by the Agency, such as a local "Special Olympics" day.
            iii) The name of a friend who is a co-worker at the Agency. Obtaining permission from that person before sharing is good practice.
         b) Examples of information that are inappropriate to share on social media include:
            i) The name of an Individual receiving services from the Agency.
            ii) Any Protected Health Information, or PHI (which includes facial images or videos of Individuals being served).

         Employees are further encouraged to portray themselves in a professional manner on any social media.
      2) **Friending/Connecting/Linking**. In general, employees should not "friend", "link", "follow", "or otherwise connect to any Individual, including any parent/guardian of an Individual, being served by CCBDD on any social media. The Agency expects employees to maintain an acceptable professional boundary with Individuals being served.
      3) **Messaging**. Employees must not use social media for Agency-related communications regarding an individual served. Employees are reminded that all Agency-related communications are subject to public records disclosure.
3) **Social Media and Workplace Harassment.** Harassing communications about coworkers on social media can constitute workplace harassment, even if done outside of the office and/or outside work hours. If you feel that you are the target of workplace harassment, report according to the anti-harassment policy.

# *2500.04.03 Portable Computing Devices*

**POLICY**
Employees who meet eligibility criteria may either be issued agency-owned smartphones and tablets, or use their personally-owned smartphones and tablets to access the organization's IT resources. Employees who are permitted to use either an employee-owned device or an agency-provided device must follow all guidelines in this policy.

**AUDIENCE**
All Staff

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.312(b) Standard: Audit Controls
45 CFR § 164.312(c)(1) Standard: Integrity
45 CFR § 164.312(d) Standard: Person or entity authentication
45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation Specifications
45 CFR § 164.312(a)(2)(iv) Encryption and decryption
45 CFR § 164.308(a)(5)(ii)(D) Password Management
45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software

**PROCEDURES**
**EMPLOYEE-OWNED MOBILE DEVICES**
1) **Agreement**. Employees must follow the organization's procedures for enrollment of their mobile device, including signing the Employee-Owned Mobile Device Agreement.
2) **Training**. The IT Staff will provide training, as necessary, to employees on how to implement the security features required while using these devices.
3) **Personal Use of Phone/Data Backup**. The employee agrees to accept responsibility to back up personal applications and data.
4) **Text Messaging**. Text messaging, since it is generally an insecure method of communication, must never contain PHI such as names of individuals served, diagnoses and interventions. Secure, encrypted email or texting is the preferred method of communication of messages that contain PHI. Text messaging is permitted when communicating appointment times.
5) **Email**. Email is the only application permitted to be used when on the Board's network.
6) **Audit**. Random audits to ensure compliance with this policy may be conducted by the Information Technologies Department. Employees must surrender the device for audit. Employees failing to comply with this policy may lose access to the CCBDD network resources through a mobile device.
7) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Policy 2500.04.05 Security Incident Response and Reporting.
8) **Permission Granted for Remote Lock/Wipe**. Employee grants the IT Department permission to perform a remote-lock, remote-wipe and/or geo-location of a device. Employee understands and accepts that the IT Department may perform a remote-lock or remote-wipe if employee's supervisor makes a written request to the Human Resources Department.
9) **Use of Device by Other People.** Employees using personal devices under this policy are responsible for controlling and/or managing the access and/or use of their device by other people including family members and friends. Employees will be held accountable for any actions performed by others who the employee permits to use the device.
10) **Replacing a Device**. Prior to replacing/upgrading a device, employees must first remove any or the organization's data prior to returning/selling/disposing of their current device.
11) **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.
12) **Discovery and other Legal Processes**. In case of legal action, personal devices used for agency business are subject to e-discovery. Users are responsible for bringing or sending the mobile device to the IT Department and giving the necessary device access codes when notified that the device is needed for e-discovery purposes.
13) **Termination and/or Suspension from Employment.** Upon termination of employment, employee agrees to provide the device to the IT department who will remove all agency data and disable access to the organization's IT resources. At the discretion of the organization, employees who are placed on administrative

leave will have access suspended until their return to work.

**AGENCY-PROVIDED MOBILE DEVICES**

1) **Eligibility Criteria and Signed Agreement**. Agency management will evaluate, on an individual basis, the eligibility of employees to use agency-owned mobile devices. Employees who wish to use an agency-owned mobile device must sign the Agency-Owned Mobile Device Agreement.
2) **Training**. The IT Staff will provide training, as necessary, to employees on how to implement the security features required while using these devices.
3) **Text Messaging**. Text messaging, since it is generally an insecure method of communication, must never contain PHI such as names of individuals served, diagnoses, and interventions. Secure, encrypted email is the preferred method of communication of messages that contain PHI. Text messaging is permitted when setting appointments.
4) **Email**. Email is the only application permitted to be used when on the Board's network.
5) **Reporting of Loss or Theft**. Loss of a smartphone containing PHI is a security incident and should be reported within 24 hours per Policy 2500.04.05 Security Incident Response and Reporting.
6) **Proper Use.** Agency-owned mobile devices must generally be used for agency-related purposes. *Minimum* personal use is permitted, such as checking weather or making a brief personal call.
7) **Use of Device by Other People Not Permitted.** Employees using agency-owned mobile devices under this policy must not allow anyone to use agency-owned mobile devices who is not permitted to use these devices under this policy.
8) **Agency-Owned Mobile Devices May Not Be Sold, Transferred, Disposed of, Recycled or Damaged.** Employees must not sell, transfer, dispose of, recycle, or intentionally or recklessly damage agency-owned mobile devices.
9) **Sanctions for Violations**. Employees who violate any of the requirements of this policy will be subject to disciplinary action.
10) **Termination and/or Suspension from Employment.** Upon termination of employment or upon administrative leave, employee agrees to return the device to the IT department.

# *2500.04.04 Employee Work at Home*

**POLICY**
Employees who are eligible to work at home must follow these procedures to ensure data security.

**AUDIENCE**
All Staff
HIPAA Security Officer and Technical Staff

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software
45 CFR § 164.312(d) Standard: Person or entity authentication
45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation specifications

**PROCEDURES**
1) **Eligibility to Work at Home.** Agency management will evaluate, on an individual basis, the eligibility of employees to work at home.
2) **No Agency Data on Home Computer/Laptop.** Employees working at home and using their home computers/laptops for work purposes are prohibited from storing agency data on their home computers/laptops.
3) **Unauthorized Cloud Storage Prohibited.** Employees are prohibited from storing agency data on any unauthorized cloud storage service.
4) **VPN Required for Network Access.** Except as permitted by Policy 2500.04.03 Portable Computing Devices, Employees must use agency-supplied Virtual Private Network (VPN) to access the agency network. The use of third-party services from remote access is prohibited.
5) **Agency Webmail.** Employees are permitted to access, from home, agency email through web-based email (webmail).
6) **Computers and Laptops Must be Kept Up-to-Date.** Employees working from home and using a personally-owned PC must ensure that the PC is routinely patched and has functioning anti-malware installed and operating.
7) **Training.** The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required by this policy.

# *2500.04.05 Security Incident Response and Reporting*

**POLICY**
The Agency will monitor all electronic information systems for breaches of security, mitigate harmful effects of security incidents to the extent practicable, and document any such security incidents and their outcomes.

**AUDIENCE**
All Staff

**AUTHORITY**
HIPAA Privacy and Security Rules, 45 CFR § 164
45 CFR § 164.308(a)(6)

**PROCEDURES**
**Creation of Response Team, Contingency Planning and Drills**
1) **Incident Response Team.** The HIPAA Security Officer is responsible for managing security incident response and reporting. At the Superintendent's option, the Agency may appoint an Incident Response Team. The mandate to this group would be to coordinate the Agency's response to security incidents. This would include mitigation strategy, communications with law enforcement, the Individuals receiving services by the Agency and the media.
2) **Contingency Plans.** The Incident Response Team may meet on a periodic basis to develop contingency plans, such as identification of a security consulting firm, public relations firm, or legal counsel who can be contacted in the event of a serious incident.
3) **Security Incident Drills.** The Incident Response Team may conduct security incident drills to develop skills and improve performance in the event of a serious security incident.

**Security Incident Reporting and Response Procedure**
1) **Reporting Security Incidents.** Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer to report the incident.
2) **Response Procedure.** The HIPAA Security Officer and/or Incident Response Team will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident. Procedures specified in Policy 2500.01.08 Breach Reporting and Policy 2400.01.09 Duty to Report Violations and Security Incidents, Policy 2500.01.12 Mitigation will be followed as appropriate. The superintendent of the Agency will be notified and any contingency plans will be activated.
3) **Documenting Security Incidents.** In conjunction with the HIPAA Security Officer, a written report must be filed within seventy-two hours (or as soon as practically possible) of becoming aware of the incident. The report should include
   A) Date and time of report
   B) Date and time of incident
   C) Description of circumstances
   D) Corrective action taken
   E) Mitigating action taken

   Documentation will be kept for 6 years.
4) **Post-Incident Analysis.** The HIPAA Security Officer and/or Incident Response Team will conduct a post-incident analysis to evaluate the organization's safeguards and the effectiveness of response, and recommend to management any changes they believe appropriate.

# APPENDICES

## Appendix A – HIPAA Security Officer Job Description

**REPORTS TO:** Superintendent

**GENERAL PURPOSE:**
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 Individual, provider, employee, and business information in compliance with organization policies and standards.

**DUTIES:**
1) Document security policies and procedures created by the information security committee/council.
2) 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.
3) Initiate activities to create information security awareness within the organization.
4) Perform information security risk assessments and act as an internal auditor.
5) Serve as the security liaison to clinical administrative and behavioral systems as they integrate with their data users,
6) Implement information security policies and procedures.
7) Review all system-related security planning throughout the network and act as a liaison to information systems.
8) Monitor compliance with information security policies and procedures, referring problems to the appropriate department manager.
9) Coordinate the activities of the information security committee.
10) Advise the organization with current information about information security technologies and issues.
11) Monitor the access control systems to assure appropriate access levels are maintained.
12) Prepare the disaster prevention and recovery plan.

**QUALIFICATIONS:**
Information security certification, such as the CISSP, is preferred.

# Appendix B – Facility Security and Access Plan

# Appendix C – Miscellaneous

**POLICY 1330 HIPAA Assignments and Documentation**
HIPAA Privacy Officer: Kathy Booth
HIPAA Security Officer: Tom Casperson
Staff person to receive HIPAA Complaints: Kathy Booth
Staff person to provide access to Individual records: Sharon Richmond
Staff person to receive requests for amendment of Individual records: Sharon Richmond
Staff person to answer questions about HIPAA policies and procedures: Kathy Booth

**Designated Record Set:**
All information in Gatekeeper software
All information relating to Individual served in Intellivue imaging software
--Archived records in paper format

# Appendix D – Change Log and Formatting Notes

**Formatting Notes**

1) The abbreviation CCBDD is used for the abbreviated Agency name throughout the document. A global replace for your preferred abbreviation is recommended.
2) The hyperlinks throughout the policy manual are best utilized with an online version of this manual. It can be saved either as a PDF or a HTML web page, which provides easy online access to all staff. If saved in HTML format it can be viewed in a web browser.
3) The Style "Heading 1" is used for Policy titles. A Microsoft Word bookmark is placed at the beginning of each Policy Title, and at beginning of certain key terms in the definitions page. It is essential that these bookmarks remain intact so that the hyperlinks to operate properly. To avoid deleting these bookmarks, it is best to set Word Options as follows. In the "Advanced" section, under "Show Document Content", select "Show Bookmarks".
4) The Table of Contents on the following page is a Microsoft Word "TOC" field, which can be updated by selecting the table of contents and pressing the F9 key. This will recreate the table of contents (policy names, page numbers) based on your changes.

**Change Log**

| Date | Policy | Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

# Employee-Owned Mobile Device Agreement

I, _____, have read, understand, and agree to abide by the requirements of Policy 2500.04.03 Portable Computing Devices (and any updates to the Policy). I agree to the following:

- I agree to complete all necessary training regarding implementing the security features of my mobile devices.
- I accept responsibility to back up personal applications and data on my mobile device(s).
- I agree to report the loss of a device containing PHI within 24 hours in accordance with Policy 2500.04.05 Security Incident Response and Reporting.
- I accept responsibility for any actions performed on my device(s) by others whom I permit to use the enrolled device(s).
- I agree to follow all procedures concerning the removal of the organization's data prior to returning/selling/disposing of my mobile device(s).
- I understand that I may be subject to disciplinary action if I access the agency's network with my mobile device(s) without following all requirements specified in Policy 2500.04.03 Portable Computing Devices.
- Upon notification, I agree to provide my enrolled mobile device(s) to the IT Department and provide all necessary access codes for e-discovery purposes and/or compliance audits.

_____ _____

Employee Name (please print) Employee Signature

_____

Date

# Agency-Owned Mobile Device Agreement

I, _____, have read, understand, and agree to abide by the requirements of Policy 2500.04.03 Portable Computing Devices (and any updates to the Policy). I agree to the following:

- I agree to complete all necessary training regarding implementing the security features of my agency-owned mobile device(s).
- I agree to report the loss of a device containing PHI within 24 hours in accordance with Policy 2500.04.05 Security Incident Response and Reporting.
- I understand that I may be subject to disciplinary action if I access the agency's network with my agency-owned mobile device(s) without following all requirements specified in Policy 2500.04.03 Portable Computing Devices.
- I understand that I may be subject to disciplinary action if I allow others unauthorized access to my agency-owned mobile device.
- I understand that I may be subject to disciplinary action if I dispose of or intentionally or recklessly damage an agency-owned mobile device.
- I understand that I may be subject to disciplinary action if I exceed acceptable personal use of an agency-owned mobile device.
- Upon termination of employment, I agree to return my agency-owned mobile device(s) to the IT department.

_____ _____

Employee Name (please print) Employee Signature

_____

Date

# Cybersecurity Policy

PURPOSE: Utilize generally accepted best practices for cybersecurity by promoting a culture of continuous learning and vigilance among CCBDD employees. We aim to strengthen CCBDD employees' ability to identify, respond to, and prevent potential cybersecurity threats effectively.
POLICY:

A. At Clermont County Board of Developmental Disabilities CCBDD, we recognize the critical importance of maintaining a secure digital environment. In order to ensure that all employees are adequately equipped to handle potential cybersecurity threats, it is mandatory for every employee to complete cybersecurity training on a yearly basis and be exposed to a monthly email test.
B. All employees are required to complete one cybersecurity training online or in-person once per year.
C. These training sessions will cover a wide range of topics related to cybersecurity, including phishing awareness, data protection, password management, and safe browsing practices. The training will be coordinated by the IT Manager.
    1. **Phishing Training Requirement:** Phishing tests will be sent once per month by the IT Manager. If an employee fails a phishing test, they are required to complete a training module.
    2. **Performance Evaluation and Support:** Regular reviews of employees' training completion records will be conducted by the IT Manager in consultation with relevant supervisors and the Human Resources department. Employees who fail to complete required training will be provided with additional support and reminders to ensure compliance.
D. **Backups:**
    1. Scheduled backups of critical data and systems Synology Active Backup for Business.
    2. Backup recovery processes will be tested at least annually.
E. **Review:**
    1. This policy will be reviewed annually to assess its effectiveness and relevance.
    2. Any necessary amendments or updates to the policy will be made in consultation with relevant stakeholders, taking into consideration the evolving nature of cybersecurity threats and industry best practices.
F. CCBDD shall not pay or comply with a ransom demand related to a ransomware incident unless it is in the best interest of CCBDD to do so and not without authorization from the CCBDD Board.
G. CCBDD shall notify the Ohio Division of Homeland Security, OHS's Cyber Integration Center, and the Ohio Auditor of State as soon as possible but not later than 7 days after discovery of a cybersecurity event that involves:
    1. A substantial loss of confidential information or integrity or availability of a CCBDD system or network.
    2. A serious impact on the safety and resiliency of CCBDD systems and processes
    3. A disruption of CCBDD's ability to engage in services

4. Unauthorized access to CCBDD's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider

H. CCBDD shall notify individuals served and employees of any data breach that may reveal PHI and provide information on recommended steps to protect from fraud or other negative effects.

By adhering to this procedure, we aim to foster a secure work environment and cultivate a strong sense of responsibility and awareness among CCBDD employees in safeguarding CCBDD's digital assets and information.