**Wood County Board of Developmental Disabilities**
**PROCEDURE**

| | | | |
|---|---|---|---|
| **Procedure #:** | 02-ALL-ALL-0845 (CP) | **Subject:** | Computer Security & Technical Safeguards |
| **Effective Date:** | 09-23-13 | **Last Revision:** | 12-11-17 |
| **Person Responsible:** | Director of Fiscal Services | | |

**Approvals/Date:** 1-4-18 1/2/17

Superintendent, WCBDD Date Department Director Date

The following definitions apply:

***Administrative Safeguards*** – Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

***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.

***Encryption*** – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

***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.

***Malicious Software*** – Software, for example, a virus, designed to damage or disrupt a system.

***Physical Safeguards*** – Physical measures, policies, and procedures to protect a covered entity's electronic information system and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

***Protected Health Information (PHI)*** – Individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI shall also include "Education Records" which are records created by WCBDD or a Business Associate that are directly related to a student who is served by WCBDD.

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

***Technical Safeguards*** – The technology and the policies and procedures for its use that protect electronic protected health information and control access to it.

***Workstation*** – An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

## TECHNICAL SAFEGUARDS

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

1. **Firewalls**. Commercial-grade hardware and 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 "Enterprise Client" level of security with modifications as necessary to allow for functionality.
   C. Microsoft Security Configuration Manager and Active Directory will be used to maintain and enforce security configurations.
3. **Operating System and Application Software Patching**. Operating Systems and Application software shall be patched regularly on both servers and workstations. Auto-update functionally may be employed to 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 guests OS's.
   D. Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations.
   E. Use separate logon credentials for each virtual server.
5. **DNS Filtering**. This shall be employed to reduce access to unsafe websites and to reduce phishing attacks, using Open DNS 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.
   E. These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
7. **Email**. For transmission of PHI, secure encrypted email 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 board shall employ the framework, detailed in NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*. Specifically, the board:
   A. should consider solutions that use existing system features (such as operating system features) and infrastructure
   B. should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments
   C. should select appropriate user authenticators for storage encryption solutions
   D. should implement measures that support and complement storage encryption implementations for end user devices
9. **Transmission Security.** For data in motion, the HIPAA Security Officer will 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:
   A. NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
   B. NIST 800-77, *Guide to IPsec VPN's*
   C. NIST 800-113, *Guide to SSL VPN's*
   D. Other FIPS 140-2 validated processes
10. **Appropriate Audit Controls in Board-Use Software.** Software used by board 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 criteria 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 county board. The HIPAA Security Officer shall be responsible for implementation and ongoing monitoring/auditing of the software as specified in Procedure 02-ALL-ALL-0580 (CP) Computer Usage under the Electronic Signatures section.
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 Procedure 02-ALL-ALL-0580 (CP) Computer Usage.
13. **Integrity Checks**. Automated integrity checks should be run on server data periodically. Any problems should be reported to the HIPAA Security Officer for corrective action.

## MALICIOUS SOFTWARE PROTECTION

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

1. The HIPAA Security Officer will insure that the computer network be protected from malicious software using a multi-layered defense strategy.
   A. Appropriately configured, commercial-grade firewall as discussed above in the Technical Safeguards section of this procedure.
   B. Centrally managed and updated anti-virus software.
   C. DNS filtering service to limit connection to malicious sites, phishing attacks, and botnets per the Technical Safeguards section of this procedure.
   D. Patching of operating system and application software per the Technical Safeguards section of this procedure.
   E. Monitoring system logs per the Audit Control and Activity Review section of Procedure 02-ALL-ALL-0656 (AD) Maintenance of HIPAA Required Documentation.
2. Special procedures will be used, if appropriate, for any users who routinely access on-line banking accounts.

## SECURITY AWARENESS PROGRAM

The board will conduct an ongoing security awareness quiz and general orientation program to train and refresh staff on the board's security policies and procedures. Priority topics shall include recognizing and avoiding malicious software, avoiding "social engineering" ploys, using passwords effectively, and adhering to workstation use policies and procedures.

1. The HIPAA Security Officer shall develop, and maintain, a security training program for new employees. This should include, at a minimum:
   A. Password policies and procedures
   B. Recognizing and avoiding malicious software
   C. Understanding email attachments
   D. Safe web browsing practices
   E. Dangers of downloading files from in the internet
   F. Understanding of "Social Engineering" and how to recognize such ploys
   G. Knowledge of Workstation Use Policies and Procedures
   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 offered 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. New and "hot" information from email advisories, online IT security news sites, and periodicals
   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.

## DEVICE AND MEDIA DISPOSAL AND RE-USE

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

1. **Media Disposal Handled by HIPAA Security Officer**. As specified in Procedure 02-ALL-ALL-0580 (CP) Computer Usage, board employees are prohibited from storing Protected Health Information on the Board'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 board requires that at a minimum, data from electronic media should be "cleared", that is, protected against a robust keyboard attack but not necessarily against a laboratory attack.
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 and Floppy Disks**. Hard drives and floppy disks should be reformatted prior to disposal or re-use.
   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)
   1. Date Conducted
   2. Conducted By
   3. Phone #
   4. Validated By
   5. Phone #

G. Sanitization Method used

H. Final Disposition of Media (Disposed/Reused Internally/Reused Externally/Returned to Manufacturer/Other)

References: 42 USC §§ 1320-1320d-9
42 CFR Parts, 160, 162, 164
45 CFR Part 164; 164.308(a)(5); 164.310(d)(1); 164.312(c); 164.312(d); 164.312(e)
NIST Special Publication 800-52; NIST 800-77; NIST 800-88; NIST Special Publication 800-111; NIST 800-113
Federal Information Processing Standards (FIPS) 140-2

Procedures: 02-ALL-ALL-0658 (AD)
02-ALL-ALL-0580 (CP)