Wood County Board of Developmental Disabilities
PROCEDURE

Procedure #:	02-ALL-ALL-0580 (CP)	**Subject:**	Computer Usage
Effective Date:	04-03-00	**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:

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.

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.

Password – Confidential authentication information composed of a string of characters.

Portable Device – A small type of a computing device, including but not limited to, laptops, netbooks, tablets, phones, USB drives, external hard drives, and like devices.

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.

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.

WORKSTATION USAGE

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

1. **System 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 we serve: their treatment, care coordination, documentation, billing, financial accounting, internet access for matters such as access do 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 Workstations, 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 time.
   B. At other times, personal use should be limited to brief access such as quickly checking the weather forecast.
   C. Workstations must never be used for any activity that would be embarrassing to the board if it became public. It is difficult to provide a complete list of such activities; a partial list includes:
      1. Downloading or viewing pornographic, racist, profane or otherwise objectionable material
      2. Conducting conversations of a sexual nature of relating to an illicit affair
      3. Relating to any illegal activity
      4. Political activity
      5. Operating a business
   D. Personal use of Social Networking tools, such a Facebook, Twitter, LinkedIn, MySpace and others is detailed separately.
   E. Employees are discouraged from staying logged in to social networking sites, instant messaging sites/tools, and their personal email except on their own time (i.e. lunch and/or breaks).
3. **Email Use**. Employees with board email accounts should check email daily. Board email accounts in general are to be used for board purposes only. Email should be written in professional manner and should be courteous respectful. Other policies when using email:
   A. Use of email internally is acceptable for transmitting PHI. Be aware that email to outside parties is not secure and must not be used to transmit 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 board.
   C. Employees should recognize that email are considered a public record and subject to disclosure to the general public.
   D. For personal matters, employees must use a personal account such as Gmail or Yahoo mail.
      1. In the event that any board email is received on a personal account, the employee must forward to the employee's board account so that it is entered into the public record.
      2. In the event that a personal email is received on a board 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, CD's, DVD's or portable hard drives, or transmit via email or fax or other method, any board confidential information or Protected Health Information on board computer system, except when specifically authorized by the HIPAA Security Officer for board purposes.
5. **All Usage is Logged**. The board reserves the right to monitor all usage of board workstations, through the logging and storage of all activity, including all emails sent or received, websites browsed, and other activity, including any personal use of board computers. All logs of employee activity are property of the board.
6. **Data Storage**. All data must be stored on the server or OneDrive. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the users Office 356 OneDrive. Any data found on workstations may be deleted without notice. No data on workstations is backed up.
7. **Duplication of Copyrighted Material Prohibited**. No employee may duplicate copyrighted software or other media using board equipment.
8. **Board Approved Hardware Only**. Only board 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 Technology Department.
9. **Electronic Signatures**. Employees using software that includes board-approved electronic signature capabilities shall follow all procedures specified in the Electronic Signatures below.

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. Workstations should be configured with automatic logoff capability so that they will become inaccessible after 10 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 Technology Department.

5. Board servers are secured with a strong password (see "User IDs and Passwords" below).

USER IDs AND PASSWORDS

1. Each employee is assigned a unique User ID and Password. Employees must only use their User ID to access board systems – and employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attribute 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.
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 will be required to change all passwords every 6 months.
5. 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.)

ELECTRONIC SIGNATURES

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

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 as described in this procedure.

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 procedure, shall use additional controls to ensure the security and integrity of each user's electronic signature:

   1. 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;
   2. Use safeguards to prevent the unauthorized use or attempted use of passwords and/or identification codes; and
   3. Test or use only tested devices, such as token or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered.

2. CREATING AND 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. Each user will sign off on Form 03-ALL-ALL-0954-Certification of Case Notes upon hire.

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 board must establish and maintain system specific procedures for any system which also satisfies other current policies.

3. AUDITING LOGGING

A. Audit Logging is controlled in each respective 3rd party program.

4. REVIEW AND APPROVAL PRIOR TO USING ELECTRONIC SIGNATURES

A. 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.

PORTABLE COMPUTING DEVICES AND HOME COMPUTER USE

Data on laptops should be encrypted and various security measures should be employed with employee-owned PDAs.

1. **Encryption on Laptops and Other Portable Devices**. Employees who use board provided laptop computers, smartphones, or other portable computing devices containing PHI shall use the encryption features to reduce the impact of disclosure in the event that the device is lost or stolen. The IT staff will use an encryption solution as detailed in Procedure 02-ALL-ALL-0845 (AD) Computer Security and Technical Safeguards.

2. **Lost Devices.** Employees must immediately report lost or stolen devices to their supervisors and the HIPAA Security Officer in accordance with Procedure 02-ALL-ALL-0686 (AD) HIPAA Security Procedure for Electronic Protected Health Information (EPHI) for Administrative Staff.
3. **Employee-Owned Portable Computing Devices**. Employees may use their personal smartphones or other portable devices to organize board activities. Storing PHI on employee-owned portable devices is prohibited. Due to the convenience of many portable devices having cameras available, personal devices may be used to capture pictures/videos of board activities. However, any images/videos collected must be forwarded directly to the Public Relations Coordinator, and employees may not use any images/videos which include individuals served in any way, which includes forwarding by text message, printing, any social media, etc. See **Sharing of Work-Related Activities** under Social Media Use Via Any Portable Devices below.
4. **Work at Home and Use of Employee's Home Computer**. Employees working at home and using their home computers for work purposes in general are prohibited from storing PHI on their home computers. Employees **must** consult with the HIPAA Security Officer regarding safeguards prior to working on any documents with PHI on their home computers.
5. **Training**. The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required while using these devices.

ASSISTIVE TECHNOLOGY

The Technology Department will provide and assist with set up of technology solutions for end-users and individuals we serve with physical, cognitive or speech disabilities.

COMPUTER VIRUS PROCEDURE

1. The Technology Department annually upgrades the Anti-Virus License for all-end users.
2. Office 365 is set up to run virus scans continuously on all incoming email.

COMPUTER EMAIL

1. The Technology Department configures Office 365 to protect email from malicious threats and spam content.
2. The Technology Department maintains yearly licenses.
3. The Technology Department configures email archiving on Office 365, which allows us to archive past, present and future email into a database.

VIOLATION OF POLICY

Any violations of this procedure will be reported immediately to your immediate supervisor. Violations of this procedure may result in disciplinary action up to and including termination and/or appropriate legal action according to the Board's disciplinary policy. Before gaining access to the Internet or e-mail services, all employees will receive a copy of this procedure and sign off on form 03-ALL-ALL-0455 which states they have read, understand, and will follow this procedure. Violation of this procedure is subject to corrective action.

References:	45 CFR Part 164; 164.308(a); 164.310(b); 164.310(c); 164.312(a)(2)(iv) ORC § 9.01; 117.111; 304 OAC 5123:2-1-11; 5160-48-01
Procedures:	02-ALL-ALL-0686 (AD) 02-ALL-ALL-0845 (CP)
Forms:	03-ALL-ALL-0954

mms\procedure\cp0580