Wood County Board of Developmental Disabilities

PROCEDURE

Procedure #:	02-ALL-ALL-0843 (AD)	**Subject:**	Confidential Records
Effective Date:	09-23-13	**Last Revision:**	12-05-17
Person Responsible:	Human Resources Coordinator		

Approvals/Date: Brent Case 12/7/17

Superintendent, WCBDD Date

Department Director Date

The following definitions will apply:

Access – The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

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.

Confidentiality – The property that data or information is not made available or disclosed to unauthorized persons or processes.

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

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

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.

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

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

The WCBDD shall conform to all requirements for privacy and confidentiality set for by the State of Ohio, the federal HIPAA and FERPA laws and any other applicable law. The WCBDD shall not use or disclose PHI except in accordance with applicable requirements. The WCBDD shall maintain appropriate physical, technical, and physical safeguards.

1. All employees using records for individuals and other paperwork with PHI shall arrange these items so that PHI is not readily visible to other individuals receiving services/visitors, especially in high traffic areas such as reception area.
2. Unneeded paper documents containing PHI shall be destroyed by shredding them in personal shredders, or placing them in one of the locked bins to be shredded by a shredding vendor.
3. Any written PHI in non-paper formats, used in fax machines, should be shredded immediately.
4. When leaving for the night, all employees shall clean their desks of PHI to reduce incidental exposures to cleaning personnel with access to the facility should be placed under a confidentiality agreement.
5. Cleaning personnel with access to the facility should be placed under a confidentiality agreement.

GENERAL PROCEDURES

1. Employees shall be familiar with Procedure 02-ALL-ALL-0838 (EFM) Gypsy Lane Complex Facility Access regarding staff, individuals receiving services, parent and other visitor access to the facility.
2. Employees shall escort visitors through the premises.

SAFEGUARDS FOR ELECTRONIC PHI

1. The HIPAA policies and procedures detail physical, technical and administrative safeguards to protect electronic PHI. In addition, these policies detail some of the physical security measures for paper records.

ORAL PRIVACY

1. Employees shall be aware of safeguarding oral communications. This includes being aware of surroundings, and using appropriate volume when speaking to prevent others from overhearing conversations.
2. Employees shall refrain from holding conversations in common areas where individuals receiving services or visitors can overhear PHI.
3. Discussions concerning individuals should be done in a private area and discussions must be limited to "need to know" information for purposes of providing the best services.
4. Overhead conversations are not to be shared or repeated.
5. When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.

SAFEGUARDS FOR WRITTEN PHI

1. Control of the Original Paper Records
   A. The HIPAA Privacy Officer shall be responsible for administering the security controls for the paper record storage.
   B. Case and School records shall be kept in a locked and secured location. Employees requiring access to these records shall have a key and/or combination for the storage room or cabinet.
   C. These files shall be put away promptly when not being used.
   D. Original paper records shall not be removed from the building without the authorization of the superintendent, privacy officer or designee.
   E. Individual records shall be retained per Procedure 02-ALL-ALL-0585 (AD) Records Retention, Storage and Destruction.
2. Other Use and Storage of Paper Records
   A. Employees should minimize the use of hardcopy PHI.
   B. Personal appointment books with names of individuals being served should be safeguarded while away from the office. It is best to avoid putting last names in appointment books if possible.
   C. Hardcopy reports and redundant copies of records personally maintained should be kept in a locked file drawer.
3. Faxing Procedure
   A. When faxing a document with PHI, use a cover sheet which indicates that information is confidential, protected under state and federal laws, and not to be re-disclosed.
   B. Care should be taken to transmit fax to the proper recipient.
   C. Faxed documents should not be left at a common fax machine.
4. Printing and Copying PHI
   A. Printers and copiers used for printing of PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
   B. PHI printed to a shared printer should be promptly removed.
5. Transportation/Outside Use of Documents with PHI
   A. Caseworkers and other employees who remove documents from the facility, to conduct field work, for example, are responsible for safeguarding these documents.
   B. When leaving documents unattended in a personal vehicle, the vehicle must be locked. The documents and/or their container should not be visible and placed in the trunk.
   C. If any documents with PHI are lost or stolen, the incident should be immediately reported to a supervisor.

COMPLIANCE AUDITS/FACILITY REVIEW

1. At least annually the HIPAA Privacy Officer shall audit staff compliance with these guidelines. The audit shall consist of a walk-through of the facility, with observations recorded, such as placement of desks, location of computer equipment, any papers with PHI that would be visible to a visitor, etc. The results shall be discussed with the appropriate employee, and any appropriate actions taken.

ENFORCEMENT

1. All supervisors are responsible for enforcing this procedure. Employees who violate this procedure will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

ANNUAL REVIEW

1. These safeguards shall be reviewed and updated annually.

AUTHORIZATION

All disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization. WCBDD will use Form 03-ALL-ALL-0294 Authorization Form, which conforms with Ohio Laws, and the federal FERPA and HIPAA regulations. FERPA applies for records created for education; HIPAA applies to all other records.

1. Valid Authorization - Unless otherwise authorized by WCBDD policy and/or state or federal law operations requires specific authorization by the Individual being served or his/her legal representative. Authorizations can be requested on Form 03-ALL-ALL-0294 Authorization Form. In the event that authorizations are received on other forms, note that a valid authorization must include the following:
   A. Full Name of the individual;
   B. A specific description of the information to be released. For example, a range of dates, or category of record;
   C. The purpose or need for the disclosure;
   D. The name of the individual, person, or agency disclosing the information;
   E. Names of the individual, person, or agency to whom the disclosure is to be made;
   F. The date, event, or condition upon which the authorization expires (which can be no longer than 180 days from the date of the signing);
   G. Statement of the individual's right to revoke the authorization, an explanation of how to revoke it, and any exceptions to the right to revoke;
   H. Statement that WCBDD may not condition treatment on whether the individual signs the authorization;
   I. A statement informing the individual of the potential that information disclosed could be redisclosed if the recipient is not subject to federal or state confidentiality restrictions;
   J. Signature and date of the individual or personal representative;
   K. If the authorization is signed by a guardian or personal representative, a description of that person's relationship to the individual and authority to sign the authorization;
   L. Written in plain language.
2. Invalid Authorization - A PHI authorization is considered invalid if authorization has the following defects:
   A. Authorization is incomplete;
   B. Authorization is not dated or time has elapsed;
   C. Authorization does not contain required elements as explained above;
   D. WCBDD is aware authorization has been revoked;
   E. WCBDD is aware information is false;
   F. Authorizations to release PHI cannot be combined with other documents.
3. For authorizations presented in person for immediate release, the staff member shall verify the identity of the recipient according to Policy 01-ALL-ALL-0135 HIPAA (Identity Verification for PHI Release), after which the information may be released.
4. Proper Completion of Authorization Form by Staff - The staff person handling the request should complete the following steps, and annotate the bottom of the Form 03-ALL-ALL-0294 Authorization Form:
   A. The employee should write their name on the completed authorization form.
   B. The original signed authorization shall be saved in the individual's master record, and a copy must be given to the individual.
   C. A record of the release shall be maintained in the individual's main record, using Form 03-ALL-ALL-0484 Disclosure Log Form, detailing the following information:
      1) The date of the disclosure;
      2) The name of the entity or person who received the PHI, and, if known, the address of such entity or person;
      3) A brief description of the PHI disclosed;
      4) A brief statement of the purpose of the disclosure;
      5) If the disclosure was due to a health or safety emergency, a description of the significant threat to health or safety.
5. Retention Period for Written or Electronic Copy of Authorization - The WCBDD must retain the written or electronic copy of the authorization for a period of six (6) years from the later of the date of execution or the last effective date.
6. Revocation of Authorization - Upon instructions of revocation of authorization, WCBDD employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure.
7. Note that information from other service providers contained in the Individual's record may be released with the individual's written authorization.

References: 42 USC §§ 1320-1320d-9
34 CFR 99; 34 CFR 99.30; 34 CFR 99.32
42 CFR Part 160, 162, 164
45 CFR 164.508; 45 CFR 164.530(c)
OAC § 5123:2-1-02(I); 5123:2-1-02(I)(7); 5123:2-4-01(C)(2)(b); 5123:2-12-02(J)(2); 5123:2-15-01(C)(6); 5123:2-3-13(B)
ORC § 5126.044
01-ALL-ALL-0135
02-ALL-ALL-0585(AD); 02-ALL-ALL-0838 (EFM)

Forms: 03-ALL-ALL-0294; 03-ALL-ALL-0484

mms\procedure\ad0843