Wood County Board of Developmental Disabilities

PROCEDURE

Procedure #:	02-ALL-ALL-0656 (AD)	**Subject:**	Maintenance of HIPAA Required Documentation
Effective Date:	04-01-03	**Last Revision:**	12-13-17
Person Responsible:	HIPAA Privacy Officer		

Approvals/Date: Brent Chow 12/22/17
Superintendent, WCBDD Date

Department Director Date

The following definitions will apply:

Applicable Requirements – Applicable requirements mean applicable federal and Ohio law and the contracts between the WCBDD and other persons or entities which conform to federal and Ohio law.

Breach – The acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information.

Breach *excludes*:

A. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA privacy rules.
B. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.

Except for the two exclusions above, any unintentional acquisition, access, use or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at least the following factors:

A. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
B. The unauthorized person who used the PHI or to whom the disclosure was made;
C. Whether the PHI was actually acquired or viewed; and
D. The extent to which the risk to the PHI has been mitigated.

Business Associate (BA) – A person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity.

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.

Guardian of the Person – An individual appointed by the Probate Court to provide consent for and make decisions for the ward.

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.

Individual, or Individual receiving services – A person who received services from WCBDD. In the event that the individual is a minor, the term "individual" in this policy may also include the parent or guardian of the individual. In addition, in regard to any privacy rights, individual may also mean an individual's "personal representative" as it is defined under HIPAA regulations.

Parent – Parent means either parent. If the parents are separated or divorced, "parent" means the parent with legal custody of the child. "Parent" also includes a child's guardian, custodian, or parent surrogate. At age eighteen, the participant must act in his or her own behalf, unless he/she has a court-appointed guardian.

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.

HIPAA ASSIGNMENTS AND DOCUMENTATION

1. The superintendent shall designate an individual to be the Privacy Officer, who is responsible for development, implementation, enforcement, and update of HIPAA Privacy policies and procedures. The superintendent may also designate other individuals to assist, a HIPAA committee, which may include representatives from each program (e.g. administration, SSA, information systems).
2. The records covered by HIPAA and FERPA shall be detailed and documented following the procedures for the "Designated Record Set" of the HIPAA regulations.

3. HIPAA mandated records include the following:
   A. HIPAA required designations, including Hybrid entity designation if applicable, description of records in complaints, providing access to individual records, receiving requests for amendment of individual records, answering questions about HIPAA policies and procedures.
   B. Notice of Privacy Practices; see Policy 01-ALL-ALL-0139 HIPAA Privacy.
   C. Restrictions on use or disclosure of PHI agreed to by WCBDD as described in Policy 01-ALL-ALL-0127 HIPAA (Consumer Requests for Extra Restrictions on Use and Disclosure of PHI).
   D. Records of disclosures, as required by Procedure 02-ALL-ALL-0451 (SS) Confidentiality of Consumer Information.
   E. Any signed authorization as described in Procedure 02-ALL-ALL-0843 (AD) Confidential Records.
   F. All privacy-related complaints received, and their disposition, if any, as described in Policy 01-ALL-ALL-0139 HIPAA Privacy.
   G. Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Procedure 02-ALL-ALL-0686 (AD) HIPAA Security Procedure for Electronic Protected Health Information (EPHI) for Administrative Staff.
   H. Incident Reports and other documentation specified by Policy 01-ALL-ALL-0139 HIPAA Privacy.
4. Policy and Procedure Audit Trail. When created or updated, all policies and procedures will be annotated with the approval date and revision history. Current policies and procedures will be maintained in a computer file folder designated "Current P & Ps". Any previous versions will be renamed with the creation date in the file name and placed in a computer file folder designated "Archived P & Ps".
5. Updating Required Designations. The Privacy Officer, will maintain and update HIPAA Required Designations as necessary.
6. Compliance Notes. The Privacy Officer and Security Officer will maintain records of compliance activity including meeting notes, vendor contracts, and internal audit activities.
7. Internal Audit. The Privacy Officer shall conduct a periodic audit, as necessary, to insure proper maintenance of all documentation itemized in this policy.
8. See Policy 01-ALL-ALL-0110 Records Retention, Storage and Destruction for retention periods and destruction procedures.

PRIVACY COMPLAINTS

1. The HIPAA Privacy Officer shall manage this complaint process, and shall be designated in the Notice of Privacy practices as the individual to receive complaints.
2. The WCBDD will extend the provisions of Policy 01-ALL-ALL-0172 False Claims Act and Whistleblower Protections, to all individuals who file confidentiality or privacy related complaint.
3. An employee or individual should file their complaint in writing to the Privacy Officer.
4. Upon receipt of a complaint, the Privacy Officer (or the employee's supervisor or Superintendent) shall review and investigate the complaint.
5. If warranted, the Privacy Officer shall take corrective action, which may include
   A. Change of policy and/or procedure.
   B. Intervention with an employee who is not following procedures including additional training and/or sanctions.
   C. Other action as appropriate.
6. The Privacy Officer shall communicate the results of the investigation and any correction action taken to the individual filing the complaint.

The WCBDD shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with Procedure 02-ALL-ALL-0656 (AD) Maintenance of HIPAA Required Documentation.

BREACH REPORTING

1. **Breach Reporting**. 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 01-ALL-ALL-0027 HIPAA (Consumer Requests for Extra Restrictions on Use and Disclosure of PHI) 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:
      1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      2. The unauthorized person who used the protected health information or to whom the disclosure was made;
      3. Whether the protected health information was actually acquired or viewed; and
      4. 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 Procedure 02-ALL-ALL-0656 (AD) Maintenance of HIPAA Required 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 HIPAA Security Officer 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);
      1. In the event of an urgent situation, the board may use telephone, email or other means to immediately notify individuals of the breach.
      2. Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following:
         a. A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known
         b. A description of the types of unsecured protected health information that were involved in the breach
         c. Any steps that individuals should take to protect themselves from potential harm resulting from the breach
         d. A brief description of what the board is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
         e. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address
      3. Send the primary breach notification to
         a. 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
         b. Parent, guardian, or HIPAA Personal Representative of the Individual in the event the individual is a minor and/or not competent to make decisions
         c. 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
      4. 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):
         a. In the event that fewer than 10 individuals, the HIPAA Security Officer shall research updated address and/or phone number and make best efforts to inform those individuals by either phone or mail
         b. In the event that 10 or more individuals are not reachable by first class mail,
            i. A toll-free phone number shall be established, and staffed with operators, for at least 90 days
            ii. A notice shall be conspicuously placed on the board's website home page with details of the above details on the breach plus the phone number
   B. Notify the news media if more than 500 individual records are involved in the breach.
      1. Under direction of the board superintendent, a press release shall be prepared detailing the information in section 3A2 above, and other relevant information.
      2. Upon approval of the board 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 Department of HHS regarding the breach
      1. 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 website
      2. For breaches involving fewer than 500 individuals, a log including at a minimum the information included on the notice to individuals detailed 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 website.
4. **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 board is responsible for issuing the notice detailed in this policy.
5. **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 board 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.
6. **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 board should have become aware if it exercised reasonable diligence.

ANNUAL SECURITY EVALUATION

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

1. On an annual basis, the HIPAA Security Officer will evaluate the security measures employed by WCBDD. This review may be conducted internally, or upon the HIPAA Security Officer's recommendation and approval by the superintendent and/or board,

contracted to an outside firm. Appropriate types of evaluations may include:

A. Penetration tests.
B. Vulnerability analyses.
C. Audits of policies and procedures to verify that they comply with applicable regulations.
D. Audits of WCBDD practices to verify that personnel are following the written policies.
E. 3rd party code reviews and/or information assurance engagements.

2. The evaluation shall be conducted and the results documented. Weaknesses should be identified and any recommendations prepared.
3. The HIPAA Security Officer shall submit their report to the superintendent and/or board including any recommendations.
4. The results of the review will be documented, and documentation shall be retained for 6 years.
5. A security evaluation should additionally be conducted with the introduction of new technology, such as wireless access, instant messaging, new smartphones etc., in response to newly recognized risks, or other event which would likely impact overall system security.

AUDIT CONTROL AND ACTIVITY REVIEW

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.

1. **System Activity Logs**. Activity logs shall be enabled at the following levels:
   A. Operating System (Windows Server). Audit Policy should be set to log logon events, account management events, policy changes, and system events as appropriate based on best practices, consistent with OS and System Software configuration specifications detailed in Procedure 02-ALL-ALL-0845 (CP) Computer Security and Technical Safeguards.
   B. Firewall Hardware and Software. Logs should be enabled to track inbound and outbound activity, configured based on best practices.
   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 an individual designated by him/her.
3. **Quarterly Audit of PHI Access**. A review of system activity will be conducted on at least a quarterly basis. The HIPAA Security Officer shall design an audit strategy to identify probably or anticipated violations. Suspicious and/or inappropriate activities include but are not limited to:
   A. Access by individuals 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. Websites 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 Information System Officer, operating system, system software, and firewall logs will be regularly monitored to detect suspicious or unusual system activity, with corrective action taken as suspicious activity is identified. This responsibility may be delegated or contracted. The use of automated tools is preferred.
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.

References: 34 CFR Part 99
42 USC §§ 1320-1320d-9
42 CFR Parts 160, 162 and 164
45 CFR Part 164; Subpart D; 164.308(a)(1); 164.308(a)(5); 164.312(b); 164.400; 164.402; 164.404; 164.406; 164.408; 164.410; 164.412; 164.414; 164.508(b)(6); 164.512(i)(2); 164.520(e); 164.522(a)(3); 164.524(e); 164.526(f) 164.528(d); 164.530(d); 164.530(j);
OAC § 5101:3-3-20(L); 5101:3-40-01; 5123:1-2-02(J)(8); 5123:1-2-08(R); 5123:1-2-11(P); 5123:2-1-02(I)(7); 5123:2-15-01(C)(6); 5123:2-15-10(G)(2)
ORC § 5123:2-1-02(I); 5123:2-1-12; 5123:64(A); 5126.044(E)

Policies: 01-ALL-ALL-0027; 01-ALL-ALL-0172

Procedures: 02-ALL-ALL-0656(AD); 02-ALL-ALL-0845(CP)

mms\procedure\ad0656