Wood County Board of Developmental Disabilities

PROCEDURE

Procedure #:	02-ALL-ALL-0686 (AD)	**Subject:**	HIPAA Security Procedure for Electronic Protected Health Information (EPHI) for Administrative Staff
Effective Date:	04-20-06	**Last Revision:**	09-23-13
Person Responsible:	HR Coordinator		

Approvals/Date:

Superintendent, WCBDD — Date 11/20/13

Department Director — Date 11/19/13

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.

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.

Employee – Any person employed by the board, volunteers, board members, and other persons whose conduct, in the performance of work for the DD Board, is under the direct control of the DD Board, whether or not they are paid by the DD Board.

Facility – The physical premises and the interior and exterior of a building(s).

Incidental Disclosure – An unintentional disclosure of PHI, that occurs as a result of a use or disclosure otherwise permitted by the HIPAA Privacy rule. An incidental disclosure is NOT a violation of the Privacy rule. However, in order for incidental disclosures to not be a violation, the covered entity must be in compliance with the requirement for implementation of the minimum necessary principle, and also in compliance with the requirement to implement physical, technical, and administrative safeguards to limit incidental disclosures.

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.

Security Incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations 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.

Facility Security and Access Control

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

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
    E. Individual Paper Records

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 Individuals** – Any staff who sees an unauthorized, unescorted person in the facility, except for incident shall be reported to the HIPAA Security Office and/or police.

Security Incident Response and Reporting

The WCBDD 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.

1. **Creation of Response Team, Contingency Planning and Drills**
    a. The HIPAA Security Officer is responsible for managing security incident response and reporting. As part of a pro-active management process, he or she may recommend to the Superintendent assignment of individuals for an incident response team. The mandate to this group would be to coordinate the Board's response to security incidents. This would include mitigation strategy, communications with law enforcement, the individuals receiving services from the Board and the media.
    b. 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.
    c. The incident response team may conduct security incident drills to develop skills and improve performance in the event of a serious security incident.
2. **Security Incident Reporting and Response Procedure**
    a. Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer to report the incident.
    b. 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 01-ALL-ALL-0139 HIPAA Privacy and this procedure will be followed as appropriate. The Superintendent of the Board will be notified and any contingency plans will be activated.
    c. 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:
        i. Date and time of report
        ii. Date and time of incident
        iii. Description of the circumstances
        iv. Corrective action taken
        v. Mitigating action taken

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

Duty to Report Violations and Security Incidents

Confidentiality of individual information, and the computer security required to protect information regarding individuals receiving services is taken very seriously at WCBDD. Employees are required to follow all rules in these policies and procedures. Any employee who becomes aware of a violation of either confidentiality or computer security rules is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

1. Employees Duty to Report Violation - Any employee observing a violation of any of the Confidentiality Records policies and procedures and Computer Security procedures is to report the violation to his/her supervisor. Failure to report a Privacy Violation is in itself a disciplinable offense.
2. Investigation - The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer shall, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, individuals receiving services, or others, and/or review of computer or paper audit trails.
3. Procedure for Security Breach - For security breaches, the Privacy and/or Security Officer will follow any procedures detailed in Policy 01-ALL-ALL-0139 HIPAA Privacy.
4. Procedure for Privacy Violation - For Privacy Violations, the Privacy Officer will follow procedures within this procedure.
5. Filing of Written Report by Privacy and/or Security Officer - A written incident report will be written by the Privacy and/or Security Officer. It will be filed
    a. In the Privacy Officer's Privacy Violations file
    b. In the employee's personnel file
6. Employee Discipline, if appropriate, will be taken and documented in accordance with Policy 01-ALL-ALL-0064 Progressive Discipline/Corrective Action.
7. Post-Incident Review - A post-incident review will be conducted by the Privacy and/or Security Officer, with any corrective action taken, such as a change in policy, additional training, or other appropriate action.

References:
45 CFR Part 164
45 CFR Part 164.308(a)(6)
45 CFR Part 164.310(a)(1)
45 CFR Part 164.530(e)(1)
NIST SP 800-66
01-ALL-ALL-0064
01-ALL-ALL-0139

mms\procedure\ad0686