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

| | | | |
|---|---|---|---|
| **Procedure #:** | 02-ALL-ALL-0846 (CP) | **Subject:** | Employee System Access and Termination |
| **Effective Date:** | 09-23-13 | **Last Revision:** | 12-11-17 |
| **Person Responsible:** | Director of Fiscal Services | | |
| **Approvals/Date:** | Brent Ashe 1-11-18 | Steve Foster 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.
***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.

**EMPLOYEE SYSTEM ACCESS AND TERMINATION PROCEDURES**

System access will be granted to employees in a manner consistent with the HIPAA Privacy laws and other state regulations, including specific policies for access control, granting access to new staff and staff with assignment changes, handling staff terminations, password selection, maintenance and use, and access to the system in the event of an emergency.

**AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS**

1. The HIPAA Security Officer shall coordinate with the Privacy Officer to maintain and document a current "minimum necessary" analysis, per the Minimum Necessary section of Procedure 02-ALL-ALL-0660 (AD) HIPAA Privacy Procedure for Protected Health Information (PHI) for Administrative Staff, which identifies the classes of persons (job descriptions) and the categories of Protected Health Information which they need access to.
2. The HIPAA Security Officer shall utilize the security capabilities of the various network and application software systems at the board and develop role-based "Access Profiles" for these different job descriptions. Vendors will be contacted for any enhancements necessary for appropriate implementation of these access profiles.
3. The authority to grant access to information systems rests with the superintendent and is delegated to the human resources department. Implicit in a hiring decision is the provision of access to the information systems necessary for the job, as determined above based on the minimum necessary analysis and the Access Profiles.
4. In certain situations, such as when employees are assigned special projects, information access may be required beyond what the job description would dictate. In these cases, the HIPAA Security Officer, after any necessary consultation with the management staff at the board, shall have the authority to grant access to information systems which go beyond the standard Access Profiles described above. Access should be terminated when the need for access is completed.
5. The HIPAA Security Officer shall maintain an updated, inventory of employees with access to PHI and the access rights which are granted.
6. On an annual basis, the HIPAA Security Officer shall audit the access controls to verify that the above policies have been implemented properly and consistently. Such an audit could include verification that recently terminated employees no longer have access, a review of access for employees with job changes in the previous year, and a random sampling of other employee access authorization. Based on the results of this audit, the HIPAA Security Officer shall adjust policies and/or staff training as appropriate.

**SYSTEM AND FACILITY ACCESS FOR NEW HIRES**

1. Supervisors and/or the human resources department shall direct requests for access to information systems shall be directed to the HIPAA Security Officer or his/her designee. The HIPAA Security Officer shall verify with the human resources department in the event of any question regarding the accuracy of the job assignment.
2. The HIPAA Security Officer will assign new hires requiring computer access a unique network User ID and password, and/or User IDs and passwords for other application systems. Security settings appropriate for the individual will be assigned in accordance with this policy, as described above.
3. The HIPAA Security Officer shall communicate the User IDs and passwords in a manner which does not compromise security by revealing the passwords to another person.
4. As described above, the HIPAA Security Officer will maintain documentation of system access rights.
5. The HIPAA Security Officer will configure a User Data Area on the Server to provide data storage space for the employee. All data is to be stored on the server and not on individual workstations.
6. Employees will receive Security Awareness Training, in the manner chosen by the HIPAA Security Officer, in accordance with the Security Awareness Program section of Procedure 02-ALL-ALL-0845 (CP) Computer Security & Technical Safeguards. In addition, new employees should receive a written copy of Procedure 02-ALL-ALL-0580 (CP), and they will sign written acknowledgement that they understand and will adhere to all policies and procedures. This will be maintained in the employee personnel file.

**PASSWORDS AND PASSWORD MANAGEMENT**

1. **Password Complexity**. Network policies and procedures shall be established enforce password complexity as follows: 8 character minimum, minimum of 1 upper case letter, 1 lower case letter and 1 digit.
2. **Lockout**. The system shall lock accounts for 5 unsuccessful attempts.
3. **Password Reuse**. The system shall maintain the previous 3 passwords and prohibit re-use of any of these recent passwords.
4. **Password Changes**. The HIPAA Security Officer shall implement a mechanism to insure that all employees change their passwords at least every 6 months.

**EMPLOYEE JOB CHANGES**

1. The Human Resource Department shall notify the HIPAA Security Officer of all job changes so that adjustments to system access can be made if necessary.

**EMPLOYEE TERMINATION**

1. On the last day of employment, employee passwords to the network and Application Software will be changed and/or their User Ids will be disabled.
2. The HIPAA Security Officer shall document the disabling of system access.
3. For involuntary terminations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the Operations Coordinator II (HR) who shall coordinate with the Technology Coordinator so appropriate precautions will be taken to insure the integrity and security of confidential board information. This could include such measures as:
   A. Physically escorting the individual off the premises after notifying him/her of the termination
   B. Disabling system access as specified above on a timely basis
   C. Requiring all staff in the individual's workgroup to change passwords
   D. Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the individual and perceived threat.

**EMPLOYEE SYSTEM ACCESS**

In the event of an emergency, such as a MUI in which immediate access to PHI is required, a staff member who does not have appropriate system permission but requires access shall contact the HIPAA Security Officer (or another staff person in that department) who will provide the necessary access on an expedited basis.

References: 42 USC §§ 1320-1320d-9
42 CFR Parts 160, 162 and 164
45 CFR Part 164; 164.308(a)(3); 164.308(a)(4); 164.308(a)(5); 164.312(a)(1); 164.314(d)

Procedures: 02-ALL-ALL-0660 (AD)
02-ALL-ALL-0580 (CP)
02-ALL-ALL-0845 (CP)

mms\procedure\cp0846