Policy Number: HC-33	Page: 1	Of: 4
Title: Security policies for HR staff & supervisors		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

SECURITY POLICIES FOR HR STAFF & SUPERVISORS

(A) 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.

Audience

Human resource department, supervisors, hipaa security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(3)

164.308(a)(4)

164.312(a)(1)

164.314(d)

164.308(a)(5) Password Management

(B)AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS

Audience: HIPAA Security Officer, Privacy Officer

1) **Minimum Necessary Analysis.** The HIPAA Security Officer shall coordinate with the Privacy Officer to maintain and document a current "minimum necessary" analysis, per Policy 1020 Minimum Necessary Policy which identifies the classes of persons (job descriptions) and the categories of Protected Health Information which they need access to.
2) **Access Profiles.** 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) **Granting Access to Information Systems**. The authority to grant access to information systems rests with board of directors 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) **Granting Access Beyond the Standard Access Profile**. 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) **Inventory of Employees with Access to PHI.** The HIPAA Security Officer shall maintain an updated, inventory of employees with access to PHI and the access rights which are granted.
6) **Annual Audit of Access Controls.** 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.

(C) SYSTEM AND FACILITY ACCESS FOR NEW HIRES

Audience: Supervisors, Human Resource Department

1) **Requests for Access to Information Systems.** 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) **Assigning User ID and Password.** 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) **Communicating User ID and Password.** 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) **Documentation of System Access Rights**. As described above, the HIPAA Security Officer will maintain documentation of system access rights.
5) **User Data Area.** 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) **Security Awareness Training.** Employees will receive Security Awareness Training, in the manner chosen by the HIPAA Security Officer, in accordance with the Policy 3040 Security Awareness Program. In addition, new employees should receive a written copy of the Policy 3080 Computer Usage, and they will sign written acknowledgement that they understand and will adhere to all policies. This will be maintained in the employee personnel file.

(D) PASSWORDS and PASSWORD MANAGEMENT

Audience: HIPAA Security Officer

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

(E) EMPLOYEE JOB CHANGES

Audience: Human Resources Department, HIPAA Security Officer

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.

(F) EMPLOYEE TERMINATION

Audience: Supervisors, Human Resource Department, HIPAA Security Officer

1) **Change Employee Password and Disable User ID.** 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) **Documentation.** The HIPAA Security Officer shall document the disabling of system access.
3) **Security Precautions for Involuntary Terminations.** For involuntary terminations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the head of human resources who shall coordinate with the Information Security Manager so that 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.

(G) EMERGENCY SYSTEM ACCESS

Audience: Supervisors, HIPAA Security Officer

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.