ACCESS TO INFORMATION TECHNOLOGY

Policy: The University shall implement appropriate safeguards to ensure that only necessary access to information technology is permitted utilizing appropriate access controls.

Rationale: To comply with 45 CFR secs.164.308(a), 164.312(a)(1), 164.312(d).

POLICY STATEMENT:

Under the HIPAA Security Rule, the University must adopt measures to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic Protected Health Information (ePHI). One method for doing so is by implementing appropriate access controls to ensure that only those who are supposed to have access to ePHI have such access.

Each HIPAA-Covered Component shall ensure that the following best practices are met with regard to access controls:

1. Members of each HIPAA-Covered Component shall be responsible for maintaining the security of their own passwords and login identification.

2. All supervisors shall be responsible for making appropriate and timely requests for activation and deactivation of user accounts for their Workforce Members.

3. All Members shall be responsible for reporting any observed breaches as outlined in the *Breach Prevention and Response Policy*.

4. Workforce Members must be vetted prior to being granted access to IT resources that store, process, have access to, and/or transmit ePHI.

5. Workforce Member access to IT resources shall be audited and re-evaluated annually or upon a job change.

Implementation

1. Each HIPAA-Covered Component shall develop a process to determine appropriate levels of authorization to access ePHI. The process shall meet the following requirements:

    - Access rights shall be granted based on business requirements.
    - Access rights shall not exceed the minimum necessary for a Member's assigned duties.

- Access rights shall be authorized and documented by the HIPAA-Covered Components Director or authorized Member.
- Access rights shall be reviewed annually or as job duties change.

Each HIPAA-Covered Component shall ensure that the following:

1. Modifications of Member access to IT resources shall be authorized and processed.

2. Security configurations shall be maintained on IT resources to restrict access to ePHI to only those Members or software programs that have been granted access in accordance with this Policy.

3. Members shall be assigned unique user identifiers (or login names) for the purposes of authenticating to IT resources.

4. Members shall not share assigned unique system identifiers (or login names) with any other person, except for authorized support purposes.

5. Members shall not share assigned passwords with any other person.

6. Anonymous access, including the use of guest and public accounts, is prohibited.

7. Member access to IT resources shall be terminated when access is no longer necessary or when determined by management.

8. The Member's manager, or manager designee, shall be responsible for making appropriate and timely requests for IT resource account deactivation.

9. The Member's manager, or manager designee, shall request IT resource account deactivation immediately if termination is due to cause or sanction.

10. The Member's manager, or manager designee, shall request IT resource account deactivation within 3 business days if termination is due to normal separation of duties.

11. A formal IT resource access termination process shall be used and shall include documentation and verification.

Reference: 45 CFR 164.308(a)
45 CFR 164.312(a)(1)
45 CFR 164.312(d)