ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

Policy: Information Technology resources of the University's HIPAA-Covered Components shall only be used in accordance with the University's Acceptable Use policies.

Rationale: In accordance with 45 CFR Part 160 and Part 164, Subparts A and C, Covered Entities and Business Associates must adopt measures to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic Patient Health Information (ePHI).

POLICY STATEMENT:

The purpose of this policy is to provide direction with regard to the use of University-owned IT equipment and software including, but not limited to, workstations, mobile computing devices, electronic communication systems and network and other business applications.

The intent of this policy is to provide information concerning appropriate and inappropriate use of University IT resources.

1. Usage of University Systems

   University systems are provided at University expense and are to be used solely to conduct University business.

   The University shall provide controls to help ensure system usage is in accordance with each Member's job duties and responsibilities.

2. Ownership of Messages, Data and Documents

   Information created, sent, received, accessed, or stored in support of University business processes is the property of the University.

3. User Responsibilities

   Members shall not tamper with or disable any security controls.

   Members may use only authorized credentials supplied to the individual to access and use University systems.

   Members learning of or reasonably suspecting any violation of a University HIPAA Security policy shall immediately report to their manager, or designee, and to the *Security Liaison*.

   Members are required to physically secure mobile computing devices in an appropriate manner whenever devices are not under direct control and monitoring by the assigned individual.

Members are to immediately report lost or stolen IT Resources to their manager, or designee, and to the *Security Liaison* in accordance with the University's HIPAA *Breach Prevention and Response Policy*.

4. Misuse of State Systems

Any use inconsistent with the University's *Acceptable Use, Information Technology* Policy is prohibited.

5. Compliance

IT resources shall be protected from misuse including, but not limited to, theft, unauthorized access, fraudulent manipulation and alteration of data, attempts to circumvent security controls, and any activity that could compromise the confidentiality, integrity or availability of data.

Any Member who violates any University HIPAA policies or underlying standards and procedures may be subject to discipline in accordance with University procedures.

6. Implementation

HIPAA-Covered Components are responsible for developing and disseminating procedures and standards governing the implementation of this policy. Such standards and procedures are therefore considered an extension of this policy and compliance is required thereto.

HIPAA-Covered Components are responsible for ensuring compliance with this policy.

HIPAA-Covered Components are responsible for making this policy available for review; obtaining a signed acknowledgment of understanding from each user; and keeping a copy of the signed acknowledgement on file.

Monitoring and oversight of the HIPAA Acceptable Use of IT Resources is the responsibility of each HIPAA-Covered Component's Security Liaison.

Reference: 45 CFR Part 160 and Part 164, Subparts A and C; P.A. 11-48 Sec. 14