DATA AUTHENTICATION & PHYSICAL SAFEGUARDS

Policy: The University shall maintain policies and procedures to protect confidential electronic data from improper alteration or destruction. This includes mechanisms to ensure that confidential electronic data have not been altered or destroyed in an unauthorized manner.

Rationale: To comply with 45 CFR 164.312.

POLICY STATEMENT:

The purpose of this policy is to provide direction with regard to data authentication and physical safeguards that should be implemented to secure ePHI.

Data Authentication

1. Authentication and authorization is required for any resource that has access to, or contains, ePHI.

2. Authentication controls shall minimally include a unique user logon and password combination.

3. The University's Information Security Office shall maintain standards for transmitting data securely.

4. Confidential electronic data shall be encrypted while stored on electronic resources.

5. Confidential electronic data shall be encrypted while in transit across a network.

6. Mail messages containing confidential electronic data shall be encrypted while in transit across a network.

7. All other confidential electronic data transmissions, e.g. client/server connections, shall be encrypted.

Physical Safeguards

1. Electronic resources with access to or containing ePHI shall be secured using physical safeguards for protection from unauthorized access.

2. Screen locks shall be activated on electronic resources.

3. Virus protection shall be installed and activated on all electronic resources containing confidential electronic data where available.

Reference: 45 C.F.R. § 164.312(c) (1)
45 C.F.R. § 164.312(c) (2)
45 C.F.R. §164.308(3) (i)
45 C.F.R. §164.308(4) (i)
45 C.F.R. §164.312(d)
45 C.F.R. §164.312 (a) (1)
45 C.F.R. §164.312 (a) (2)