UNIVERSITY OF WYOMING

HIPAA POLICY 5.4

SECURITY RULE TECHNICAL SAFEGUARDS

I. **PURPOSE:** The purpose of this policy is to ensure UW Covered Components comply with the technical safeguards required by the HIPAA Security Rule.

II. **RESPONSIBILITY:** Each UW Covered Component is responsible for implementation of policies and procedures for each area identified within this policy.

III. **ACCESS CONTROL:** Each UW Covered Component shall implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

a. **Unique User Identification (Required):** Each UW Covered Component shall assign a unique name and/or number for identifying and tracking user identity.

b. **Emergency Access Procedure (Required):** Each UW Covered Component shall establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

c. **Automatic Logoff (Addressable).** Each UW Covered Component shall implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

d. **Encryption and decryption (Addressable).** Each UW Covered Component shall implement a mechanism to encrypt and decrypt electronic protected health information.

IV. **AUDIT CONTROLS:** Each UW Covered Component shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

V. **INTEGRITY:** Each UW Covered Component shall implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

a. **Mechanism to Authenticate Electronic PHI (Addressable).** Each UW Covered Component shall implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

VI. **PERSON OR ENTITY AUTHENTICATION:** Each UW Covered Component shall implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

a. **Integrity Controls (Addressable).** Each UW Covered Component shall implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

b. **Encryption (Addressable).** Each UW Covered Component shall implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

VII. REFERENCES/APPLICABLE LAW:

a. 45 C.F.R. Section 164.310

Revised xx/xx/2015