UNIVERSITY OF WYOMING

HIPAA POLICY 5.1

SECURITY STANDARDS: GENERAL RULES

I. PURPOSE: The purpose of this policy is to ensure UW Covered Components comply with the general rules 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. GENERAL REQUIREMENTS: Each UW Covered Component must do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
d. Ensure compliance with the Security Rule by its workforce.

IV. SECURITY MEASURES: Each UW Covered Component may use any security measures that allow the UW Covered Component to reasonably and appropriately implement the standards and implementation specifications as specified in the Security Rule. In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

a. The size, complexity, and capabilities of the UW Covered Component.
b. The UW Covered Component's technical infrastructure, hardware, and software security capabilities
c. The costs of security measures.
d. The probability and criticality of potential risks to electronic protected health information.

V. IMPLEMENTATION SPECIFICATIONS: The HIPAA Security requirements throughout the Security Rule policies are identified as either required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

a. **Required:** When an implementation specification is identified as "Required" the UW Covered Component must implement that particular specification.
b. **Addressable:** When an implementation specification is identified as "Addressable" the UW Covered Component must:
    i. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

ii. As applicable to the UW Covered Component:
    1. Implement the implementation specification if reasonable and appropriate; or
    2. If implementing the implementation specification is not reasonable and appropriate:
        a. Document why it would not be reasonable and appropriate to implement the implementation specification; and
        b. Implement an equivalent alternative measure if reasonable and appropriate.

VI. MAINTENANCE: Each UW Covered Component must review and modify the security measures implemented under this policy as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measure.

VII. IMPLEMENTATION AND DOCUMENTATION OF POLICIES AND PROCEDURES: Each UW Covered Component shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

a. **Changes to Policies:** A UW Covered Component may change its Security Rule policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this policy.
b. **Documentation:** A UW Covered Component must maintain its policies and procedures to comply with the Security Rule in written (which may be electronic) form and if an action, activity or assessment is required by the Security Rule to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.
    i. **Time Limit (Required):** A UW Covered Component shall retain its Security Rule policies and procedures for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
    ii. **Availability (Required).** A UW Covered Component must make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
    iii. **Updates (Required).** A UW Covered Component must review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

VIII. REFERENCES/APPLICABLE LAW:

a. 45 C.F.R. Section 164.306
b. 45 C.F.R. Section 164.316

Revised xx/xx/2015