**UNIVERSITY OF WYOMING**

**HIPAA POLICY 5.2**

**SECURITY RULE ADMINISTRATIVE SAFEGUARDS**

**I. PURPOSE:** The purpose of this policy is to ensure UW Covered Components comply with the administrative 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. SECURITY MANAGEMENT PROCESS:** Each UW Covered Component shall implement policies and procedures to prevent, detect, contain, and correct security violations, which shall include at a minimum:

a. **Risk Analysis (Required):** Each UW Covered Components shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the UW Covered Component.

b. **Risk Management (Required):** Each UW Covered Component shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

   i. Ensure the confidentiality, integrity, and availability of all electronic PHI the UW Covered Component creates, receives, maintains or transmits.

   ii. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

   iii. Protects against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.

   iv. Ensure compliance with the Security Rule by its workforce.

c. **Sanction Policy (Required):** Each UW Covered Component shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. (See UW HIPAA Policy 3.5)

d. **Information System Activity Review (Required):** Each UW Covered Component shall implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

**IV. ASSIGNED SECURITY RESPONSIBILITY:** The UW Security Officer and each UW Covered Component's Security Officer are responsible for the development and implementation of the policies and procedures required in this policy.

**V. WORKFORCE SECURITY:** Each UW Covered Components shall implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under its information access management policies and procedures, and to prevent those workforce members who do not have access under its information access management policies and procedures from obtaining access to electronic protected health information.

a. **Authorization and/or Supervision (Addressable):** Each Covered Component shall implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
b. **Workforce Clearance Procedures (Addressable):** Each Covered Component shall implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
c. **Termination Procedures (Addressable):** Each Covered Component shall implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made under the workforce clearance procedures.

**VI. INFORMATION ACCESS MANAGEMENT:** Each UW Covered Component shall implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the Privacy Rule.

a. **Access Authorization (Addressable).** Each UW Covered Component shall implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
b. **Access Establishment and Modification (Addressable).** Each UW Covered Component shall implement policies and procedures that, based upon the UW Covered Component's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

**VII. SECURITY AWARENESS AND TRAINING:** Each UW Covered Component shall implement a security awareness and training program for all members of its workforce (including management).

a. **Security Reminders (Addressable):** Each Covered Component shall issue periodic security updates.
b. **Protection from Malicious Software (Addressable):** Each Covered Component shall implement procedures for guarding against, detecting, and reporting malicious software.
c. **Log-in Monitoring (Addressable)**: Each Covered Component shall implement procedures for monitoring log-in attempts and reporting discrepancies.
d. **Password Management (Addressable):** Each UW Covered Component shall implement procedures for creating, changing, and safeguarding passwords.

**VIII. SECURITY INCIDENT PROCEDURES:** Each UW Covered Component shall implement policies and procedures to address security incidents.

a. **Response and Reporting (Required).** Each UW Covered Component shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

**IX. CONTINGENCY PLAN:** Each UW Covered Component shall establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

a. **Data Backup Plan (Required).** Each UW Covered Component shall establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
b. **Disaster Recovery Plan (Required).** Each UW Covered Component shall establish (and implement as needed) procedures to restore any loss of data.
c. **Emergency Mode Operation Plan (Required).** Each UW Covered Component shall establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
d. **Testing and Revision Procedures (Addressable).** Each UW Covered Component shall implement procedures for periodic testing and revision of contingency plans.
e. **Applications and Data Criticality Analysis (Addressable).** Each UW Covered Component shall assess the relative criticality of specific applications and data in support of other contingency plan components.

**X. EVALUATION:** Each UW Covered Component shall perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this policy and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information. The evaluation establishes the extent to which a UW Covered Component's security policies and procedures meet the requirements of the Security Rule.

**XI. BUSINESS ASSOCIATES:** A UW Covered Component may permit a business associate to create, receive, maintain or transmit ePHI on the UW Covered Component's behalf only if the UW Covered Component obtains satisfactory assurances in the form of a written business associate contract, that the business associate will appropriately safeguard information.

a. **Business Associate Contracts:** Business Associate contracts must provide that the business associate will
    **i.** Comply with all applicable Security Rule requirements;
    **ii.** Ensure that subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and
    **iii.** Report to the UW Covered Component any security incident of which it becomes aware, including breaches of unsecured protected health information.

**XII. REFERENCES/APPLICABLE LAW:**

a. 45 C.F.R. Section 164.308

b. 45 C.F.R. Section 164.314

Revised xx/xx/2015