UNIVERSITY OF WYOMING

HIPAA POLICY 5.3

PHYSICAL SAFEGUARDS

I. PURPOSE: The purpose of this policy is to ensure UW Covered Components comply with the physical 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. FACILITY ACCESS CONTROLS: Each UW Covered Component shall implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

a. **Contingency Operations (Addressable).** Each UW Covered Component shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
b. **Facility Security Plan (Addressable).** Each UW Covered Component shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
c. **Access Control and Validation Procedures (Addressable).** Each UW Covered Component shall implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
d. **Maintenance records (Addressable).** Each Covered Component shall implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

IV. WORKSTATION USE: Each UW Covered Component shall implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

V. WORKSTATION SECURITY: Each UW Covered Component shall implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

VI. DEVICE AND MEDIA CONTROLS: Each UW Covered Components shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

a. **Disposal (Required):** Each Covered Component shall implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
b. **Media Re-Use (Required):** Each Covered Component shall implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
c. **Accountability (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
d. **Data Backup and Storage (Addressable).** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

VII. REFERENCES/APPLICABLE LAW:

a. 45 C.F.R. Section 164.310

Revised xx/xx/2015