UNIVERSITY OF WYOMING

HIPAA POLICY 3.6

BREACH

I. **PURPOSE:** The purpose of this policy is to outline the processes and procedures for determining whether the security or privacy of PHI has been compromised and to ensure compliance with notification and reporting requirements pursuant to HIPAA, as amended by the HITECH Act of 2009, as well as any other applicable Federal or State laws.

II. **INITIAL REPORT OF SUSPECTED BREACH INVOLVING PHI:**

a. All workforce members, including volunteers and students, of a UW Covered Component shall report any actual or suspected unauthorized access, acquisition, use or disclosures of PHI to the UW Covered Component Privacy and Security Officer immediately.

b. Business Associate Agreements executed by a UW Covered Component shall require the contractors to notify the UW Covered Component of any unauthorized use or disclosure by the business associate or its workforce, agents or subcontractors that violates the HIPAA Privacy or Security Rules, including any remedial action proposed or taken.

c. This policy applies to "unsecured PHI." Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. Encryption and destruction are the only two technologies currently recognized by the Secretary for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. PHI that is encrypted or destroyed is not subject to this policy regarding breach and notification.

III. **PROCEDURE:** The UW Covered Component Privacy and Security Officer is responsible for immediately notifying the UW Privacy Officer, Security Officer, Risk Management and Office of General Counsel of any reported incident that upon preliminary analysis could reasonably constitute a breach.

a. **Coordination of Investigation:** The UW Covered Component Privacy and/or Security Officer shall lead the effort to ensure that all relevant information is gathered and reported timely. If the UW Covered Component Privacy and/or Security Officer is not available, the UW Covered Component shall designate an alternate to have this responsibility.

    i. Depending on the nature of the assessment, the UW Covered Component Privacy and/or Security Officer may call upon other employees of the University to assist in the investigation or potentially recommending engaging non-University consultants, as necessary, to assist the University in its investigation or risk analysis.

    ii. The investigation may include conducting interviews to learn about the circumstances surrounding the incident, reviewing documents, and using other resources, as applicable.

b. **Presumption of Breach:** All unauthorized acquisitions, access, or impermissible uses and disclosures of PHI are presumed to be a breach unless the outcome of a risk assessment determines otherwise.
c. **Risk Assessment:** The UW Covered Component Privacy and/or Security Officer shall perform a risk assessment that includes the following:
    i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
        1. For example, did the breach involved "unsecured" protected health information?
        2. Can the information disclosed cause: "significant risk of financial, reputational, or other harm to the individual"?
    ii. The unauthorized person who used the PHI or to whom the disclosure was made;
        1. In other words, in whose hands did the PHI land?
    iii. Whether the PHI was actually acquired or viewed; and
    iv. The extent to which the risk to the PHI has been mitigated.
        1. For example, can you obtain forensic proof that a stolen laptop computer's data was not accessed?
    v. Any other relevant factors.
d. Exceptions to Breach: There is no breach if the UW Covered Component has sufficient documentation to show that the acquisition, access, use or disclosure of PHI falls into any of the following categories:
    i. **Unintentional Uses or Disclosures:** Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
    ii. **Inadvertent Uses or Disclosures:** Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
    iii. **No Retention:** A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
e. **Final Determination:** The next steps after the investigation has been completed into any suspected breach will depend on the findings.
    i. **Breach Occurred:** If there is a determination that a breach occurred, notification must be given pursuant to section IV below.

ii. **No Breach:** If the determination is made that no breach occurred, no notification is required; however, all documentation and evidence provided during the investigation must be maintained by the UW Covered Component for a period of six years.

1. **Note:** Breaches must be analyzed for possible Non-HIPAA breaches, i.e. breaches under a Wyoming state law or other applicable Federal laws, as well.

IV. NOTIFICATION: A breach will be treated as discovered by the UW Covered Component on the first day such breach is known or should reasonably have been known to have occurred by the UW Covered Component or its Business Associate, even if it is initially unclear whether the incident constitutes a breach. The type of notice required depends on the type of breach.

a. Notification to Individuals: A UW Covered Component shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

i. Timeliness: Required notification to the individual shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

ii. Contents of Notice: The notice must include, to the extent possible, the following in plain language:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

iii. **Methods of Notice:** Notice to the individual shall be provided as follows:

1. **Written notice:** In writing by first class mail to the individual's last known address; or if deceased, notification must be sent to the address of the next of kin or legally recognized personal representative. If the individual has agreed to receive electronic notice and has not withdrawn such agreement, notification by electronic mail is appropriate. Notification may be provided in one or more mailings as information becomes available.

2. **Substitute Notice:** In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
    a. **Fewer than 10 individuals:** If there is insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.
    b. **10 or more individuals:** In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:
        i. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
        ii. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
3. **Urgent Notice:** If the UW Covered Component deems the situation to be urgent, the individual/s may be notified by telephone or other means, as appropriate, in addition to providing written notice.
4. **Media if Affects More than 500 Individuals:** If the breach affects more than 500 individuals residing in a particular state, the UW Covered Component shall notify prominent media outlets serving the area.
    a. The notification shall be provided without unreasonable delay and no later than 60 calendar days after the discovery.
    b. The information provided shall be the same as set forth in IV(a)(ii).
    c. Notification to media outlets will be provided in addition to the individual notification requirements and not as a substitute.
5. **Notification to the Secretary of HHS:** The Secretary shall be notified as follows:
    a. **Breaches Affecting 500 or More Individuals:** Notification must be provided contemporaneously with notification of the individuals and in the manner specified on the HHS web site.
    b. **Breaches Affecting Less than 500 Individuals:** The UW Covered Component shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each

calendar year, provide the notification for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

c. **UW Covered Component Privacy Officer Responsible for Notice:** The UW Covered Component's Privacy Officer shall make the notification to the Secretary as required under this section.

6. **Notification by a Business Associate:** A Business Associate must notify the applicable UW Covered Component within a reasonable time, but in no case more than 60 calendar days after the date of discovery of the breach, including any available information that is required to include in the notification to the individual/s affected by the breach. Said notifications to individual/s affected by the breach will be made by the UW Covered Component pursuant to this policy.
7. **Law Enforcement Delay:** If a law enforcement official states to a UW Covered Component that a required notification, notice or posting would impede a criminal investigation or cause damage to national security, the UW Covered Component shall:
    a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
    b. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

V. ADMINISTRATIVE REQUIREMENTS

a. Training: UW Covered Components shall train all employees, volunteers or students whose functions are affected by this policy on the requirements of notification of unsecured breaches.

b. Complaints: Complaints regarding breaches of unsecured PHI and failure to follow this policy shall be made with UW Covered Component's Privacy Officer.

c. Sanctions: Employees or members of a UW Covered Component's workforce who fail to comply with these policies and procedures will be disciplined in the same manner as set forth in University of Wyoming applicable Regulations and policies and the UW HIPAA Sanctions Policy.

d. **Non-Retaliation:** A UW Covered Component shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by the HIPAA Privacy or Security Rule, including the filing of a complaint. A UW Covered Component shall not require an individual to waive their rights as a

condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

e. Documentation: A UW Covered Component shall maintain these policies and all documentation and decisions pursuant to this section for a period of six years from the date of its creation or the date when it last was in effect, or as required by state or federal law or UW Regulations, whichever is later.

VI. REFERENCES/APPLICABLE LAW:

a. 45 CFR 164.530

b. 45 CFR 164.400-414

Revised August 2015