THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

INSTITUTIONAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT POLICY - INTERIM

Number 06.09.06

Division Finance and Administration – Office of Risk Management and Compliance

Date October 10, 2024

Policy The University of Alabama in Huntsville ("University") strives to protect the confidentiality, integrity, and availability of protected health information ("PHI") by taking reasonable and appropriate steps to address the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and Alabama law for those designated health care components that engage in covered functions. This Policy guides the University's efforts to comply with HIPAA, including its privacy, security, and breach notification rules. The University reserves the right to modify any or all of this Policy without notice and at its discretion or as otherwise may be required by law.

Purpose Under HIPAA, an organization that performs both HIPAA-covered and non-covered functions may elect to become a hybrid entity. Once that election is made, only the entity's designated health care components that perform covered functions are subject to HIPAA. This policy announces the University's election as a hybrid entity, designates the health care components that perform covered functions, and establishes written procedures to secure the privacy of PHI and prevent its improper use or disclosure, in compliance with HIPAA and Alabama law.

Procedures To ensure that the University implements and maintains policies for the use and disclosure of health information in compliance with HIPAA and Alabama law, the University sets forth the following procedures.

1. Hybrid Entity Designation

The University is a single legal entity, comprised of multiple and distinguishable schools, departments, clinics, programs, and functions, some of which may conduct covered or non-covered functions under HIPAA. Accordingly, to effectively safeguard the use and disclosure of PHI and to focus its HIPAA compliance efforts on those components which engage in covered functions, the University hereby designates the following health care components ("University health care components"), which are subject to HIPAA:

- UAH Health Services
- UAH Employee Group Health Plan

Additionally, the University designates the following health care components, which are subject to HIPAA only to the extent they perform the functions of a Covered Entity or business associate (e.g., functions that involve the use and/or disclosure of PHI):

- UAH Office of Risk Management and Compliance
- UAH Office of Information Technology
- UAH Payroll Services
- UAH Human Resources
- Other University units or departments to the extent that their activities are subject to Business Associate Agreements ("BAA")
- Other University units or departments to the extent that they access and/or create PHI for research purposes
- University of Alabama System units or departments sitting by designation at UAH, including the Office of Counsel and Internal Auditing

The University will conduct periodic reviews to add or remove one or more University designated health care components. Any non-designated University component that seeks to engage in a covered function shall first seek approval from the designated HIPAA Privacy Officer. The HIPAA Privacy Officer, in coordination with the Office of Counsel, shall assess whether the component will be designated as a health care component for purposes of this Policy.

2. Privacy

University health care components will not use or disclose PHI except as permitted or required by HIPAA as provided in this Policy. Requests for exceptions to this Policy shall be reviewed by the HIPAA Privacy Officer, in consultation with the Office of Counsel.

a. General Responsibilities

Except as provided herein, University health care components will make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standard does not apply to disclosures to or requests by healthcare providers for treatment, disclosures to the individual who is the subject of the disclosure, uses or disclosures made pursuant to authorizations, uses or disclosures required by law, or disclosures to the Secretary of the Department of Health and Human Services.

Whenever an individual's authorization or opportunity to object is required by this Policy, University health care components will treat personal representatives as the individual for purposes of this Policy, as appropriate. Personal representatives are either (1) individuals with authority to act on behalf of an adult or emancipated minor in making decisions related to healthcare, or (2) executors or administrators acting on behalf of a deceased individual or the individual's estate. If adults have the authority of personal representatives and are furnishing consent for healthcare treatment for unemancipated minors, University health care components will honor the request, consent, and authorization from the adults with that authority. Minors may independently request, consent, or authorize the use and disclosure of PHI under this Policy for healthcare services for which they are legally authorized and do consent, independent of any other consent, including that of their parents or other personal representatives.

University health care components are not required to honor the requests of personal representatives if the entity has a reasonable belief that the personal representative is

abusing or neglecting the patient or if the entity, in the exercise of professional judgment, decides that it is not in the best interest of the patient to treat the person as the patient's personal representative.

University health care components will develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to PHI to carry out their duties, the categories of PHI to which access is needed, and any conditions under which they need the information to do their jobs.

b. Required Disclosures

University health care components must disclose PHI to (1) an individual who requests their own PHI or (2) the Secretary of the Department of Health and Human Services to investigate the University's compliance with HIPAA.

c. Permitted Disclosures

University health care components are permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

- *Treatment*. University health care components may use PHI for treatment, payment, or healthcare operations, except for psychotherapy notes as provided further herein.

- *Payment*. University health care components may disclose PHI to another provider for treatment activities of that provider or to another covered entity for payment activities of that entity.

- *Healthcare operations*. University health care components may disclose PHI to another covered entity for healthcare operations if each covered entity has or had a relationship with the individual and the disclosure is for a healthcare operation purpose.

- *Business associates*. University health care components may disclose PHI to a business associate if the business associate has executed a BAA with the University health care component. The following disclosures do not require BAAs: (1) to providers for treatment; (2) to health plans for payment; (3) to any entity that is merely serving as a conduit for transmission of the PHI (i.e., telephone companies); (4) incidental disclosures of PHI (i.e., janitorial staff); or (5) within an organized healthcare arrangement. University health care components must promptly report to the Designated HIPAA Officer, the HIPAA Privacy Officer, or the Office of Counsel any instances of a pattern of activity of the business associate that constitutes a material breach or violation of the business associate's obligations under the agreement so that reasonable steps may be taken to cure the breach, end the violation, or terminate the agreement.

- *De-Identified data*. There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

d. Circumstances in Which PHI May Be Shared Without Patient Consent, Authorization, or Opportunity to Object

University health care components may use or disclose PHI with no patient consent, authorization, or opportunity to object under any of the following circumstances:

- *Required by law*. University health care components may use or disclose PHI when use or disclosure is required by law.

- *Public health activities.* University health care components may use or disclose PHI for public health activities, such as preventing the spread of communicable disease, reporting adverse events for FDA regulated products, and for employers to comply with work-related illness and injury laws.

- *Reporting of victims of abuse, neglect, or domestic violence.* University health care components may use or disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

- *Health oversight activities.* University health care components may use or disclose PHI to agencies responsible for oversight of the health care system and government benefit programs.

- *Judicial administrative proceedings.* University health care components may use or disclose PHI to comply with a court order, subpoena, or other lawful process (see also Service of Process Policy).

- *Law enforcement purposes.* University health care components may use or disclose PHI for certain law enforcement purposes, as described at 45 C.F.R. § 164.512(f).

- *Family members of decedent.* University health care components may use or disclose PHI to a family member, other relative, or close personal friend who was involved in the individual's care or payment for care (not just personal representative) prior to the individual's death PHI of the deceased individual that is relevant to that person's involvement unless doing so is inconsistent with any prior expressed preference of the deceased individual made known to the University health care component.

- *Coroners, medical examiners, and funeral directors.* University health care components may use or disclose PHI to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

- *Cadaveric, organ, eye, or tissue donation.* University health care components may use or disclose PHI to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

- *Research*. University health care components may use or disclose PHI for certain research purposes, subject to the following limitations: (1) documented Institutional Review Board (IRB) or Privacy Board approval (see 45 C.F.R. § 164.512(i)(1)(i)); (2) preparatory to research (see 45 C.F.R. § 164.512(i)(1)(ii)).; (3) research on PHI of decedents (see 45 C.F.R. § 164.512(i)(1)(iii)); (4) limited data sets with a data use agreement (see 45 C.F.R. § 164.514(e)); or (5) research use/disclosure with individual authorization (see 45 C.F.R. § 164.508). Use or disclosure of any other PHI for research purposes requires patient authorization on an approved University Authorization Form. Research is subject to HIPAA privacy requirements when it is conducted alone or in conjunction with the provision of health care services by individuals who are part of a covered entity or component and involves the use or PHI, or when it is conducted using PHI from any external covered entity.

- *Workers' compensation.* University health care components may use or disclose PHI to employers and administrators for workers' compensation or similar programs. If a third-party administrator ("TPA") is utilized to help administer the University's self-insured workers' compensation plan and that TPA conducts activities covered by HIPAA, a BAA is required from the TPA.

- *Avert a serious threat to health or safety.* University health care components may use or disclose PHI to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone who can prevent or lessen the threat.

- *Specialized government functions.* University health care components may use or disclose PHI to military command authorities for military or veteran activities, to federal official for intelligence and national security activities and protective services, and to correctional institution or law enforcement official for provision of health care or for the health and safety of others.

e. Disclosures to Third Parties with Patient Opportunity to Agree or Object

Individuals shall be informed of these possible uses and disclosures of PHI and of their right to object to these uses in the University Notice of Health Information Practices. When the individual has been notified of the possible uses and disclosures of PHI and given an opportunity to agree or object, the University health care component may use or disclose PHI for any of the following:

- *Individuals (family members, friends, or others) involved in the patient's care or in payment for the patient's care.* University health care components may use or disclose PHI to share information with family, friends, or others involved in the individual's care.

- *Disaster relief*. University health care components may use or disclose PHI to share information in a disaster relief situation.

- *Facility directory.* University health care components may use or disclose PHI to include information in a facility directory.

- *Emergencies.* University health care components may use or disclose PHI for any of the above reasons, in the event the individual is incapacitated, in an emergency situation, or not available, if in the exercise of the professional judgment of the provider, the use or disclosure is determined to be in the best interests of the individual.

f. Psychotherapy Notes

Psychotherapy notes may only be used or disclosed by University health care components under the following conditions: (1) with an authorization signed by the patient; (2) without an authorization from the patient, if use and disclosure is limited to (a) use by the originator of the psychotherapy notes for treatment, (b) use or disclosure by the University in mental health training programs, or (c) use or disclosure to defend legal actions or other proceedings brought by the patient; or (3) as required by law.

g. Incidental Disclosures

University health care components are permitted, but not required, to use and disclose protected health information, without an individual's authorization, when the use or disclosure is incidental or secondary to an otherwise permissible use or disclosure, provided reasonable safeguards are in place. Incidental disclosures may include, but are not limited to, teaching rounds, sign-in sheets in clinics, and overhead pages.

h. Authorizations

Authorizations are required for all uses and disclosures of PHI not otherwise addressed in this Policy, subject to the following limitations:

- *Psychotherapy notes.* Authorization must be obtained to use or disclose psychotherapy notes, except as described herein. Compound authorizations are not permitted for psychotherapy notes or for instances in which a University health care component conditioned treatment on execution of an authorization.

- *Sale of PHI*. The sale of patient data, even if de-identified, is inconsistent with the relationship established with patients when they present for care. Therefore, the sale of patient data shall not be permitted if it is primarily for the benefit of the recipient, unless the data is required by law or for public health purposes, the data is required for research, or the data is required for analysis or other processing deemed beneficial to the covered entity. Nonetheless, authorization must be obtained for any disclosure which is a sale of PHI.

- *Criminal acts*. An employee who is a victim of a criminal act may disclose PHI to a law enforcement official if the disclosure is about the suspected perpetrator of

the criminal act and the PHI is limited to name/address, birthdate, social security number, ABO blood type, and rh factor, type of injury, date/time of treatment, and distinguishing physical characteristics. An employee or business associate of a University health care component may disclose PHI to oversight agencies if they believe the entity is engaging in unlawful conduct of which the employee has notified the entity and the entity has not responded to the employee.

Authorizations must be on an approved HIPAA compliant authorization form. All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

Individuals may revoke authorizations by submitting a written revocation to a University health care component. The revocation will not be effective for any actions taken in reliance on the authorization prior to receipt of the written revocation.

University health care components are responsible for developing processes to ensure appropriate authorizations are obtained for use and disclosure of PHI, when required, and that copies of the authorizations and any revocations are maintained for a period of six (6) years.

i. Notice of Privacy Practice

Each University health care component will provide a notice of its privacy practices containing the elements described at 45 C.F.R. § 164.520. Components must personally furnish the notice no later than the first service encounter (or as soon as practicable in emergency situations) and also must post the notice and in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice. If the component maintains a web site, the component must prominently post its notice on the web site and make the notice available electronically through the web site. Each component must make a good faith effort to obtain written acknowledgement from patients of receipt of the notice of privacy practices.

j. Patient Health Information Rights

Patients have certain rights with respect to the privacy of their PHI, including, but not limited to, the following:

- *Right to Access.* University health care components must make available in a timely manner, upon request from the individual, a copy of the individual's PHI contained in the component's designated record set, with the exception of psychotherapy notes and information compiled for legal proceedings. Access to the PHI must be in the form and format requested by the individual, including in electronic format if the records exist electronically. University health care components may impose reasonable, cost-based fees to cover the cost of copying and postage. Access may be denied pursuant to the grounds and in accordance with the processes described at 45 C.F.R. § 164.524(a)(2) and (3).

- *Right to Request Restriction on Use or Disclosure*. Individuals have the right to request that a University health care component restrict use or disclosure of PHI for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. A University health care component is under no obligation to agree to requests for restrictions. Each University health care component is responsible for developing a process to review and respond to these requests. This process shall include a method to maintain documentation of any agreed upon restrictions.

- *Right to Receive Confidential Communications*. University health care components will permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that the component typically employs.

- *Right to Request Amendment of PHI*. Individuals have the right to request an amendment to their PHI when that information is inaccurate or incomplete. If a University health care component accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, components must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. University health care components must adopt processes and procedures for handling amendment requests pursuant to the requirements described at 45 C.F.R. § 164.526.

- *Right to Accounting of Disclosures*. University health care components must, upon request of the individual, provide an accounting of disclosures of the individual's PHI by the component (or the component's business associates). The maximum disclosure accounting period is the six years immediately preceding the accounting request, subject to the limitations described at 45 C.F.R. § 164.528.

- *Right to Revoke Authorization.* An individual has the right to revoke an authorization to use or disclose his or her medical information except to the extent that action has already been taken in reliance on the authorization.

- *Right to a Paper Copy of the Notice of Health Information Practices.* An individual has the right to a paper copy of the covered entity's Notice of Health Information Practices at any time.

k. Policies and Procedures

The University and its health care components will develop and implement written privacy policies and procedures that are consistent with the HIPAA Privacy Rule. Such policies and procedures developed by University health care components should be made available to the Office of Risk Management and Compliance for review and retention.

l. Business Associate Requirements

The University requires all business associates to enter into a standard BAA using the University's approved template, or a template deemed acceptable by University counsel, to ensure compliance with the Privacy Rule under HIPAA. This agreement mandates that business associates protect the confidentiality of PHI and limit the use and disclosure of such information to what is permitted or required by law. In circumstances where the standard template cannot be used, the agreement must, at a minimum, fulfill the Privacy Rule's requirements by incorporating provisions that ensure the proper handling, use, and disclosure of PHI, and safeguard the rights of individuals regarding their health information.

m. Complaints

Each University health care component will develop and implement procedures for individuals to complain about its compliance with its privacy policies and procedures and the HIPAA Privacy Rule.

n. Anti-Retaliation

Neither the University nor its health care components will retaliate against a person for exercising rights provided by the HIPAA Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. A health care component may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

o. Mitigation

The University will take all reasonable steps to mitigate any harmful effects resulting from the improper use or disclosure of PHI in violation of its policies, procedures, or applicable legal requirements, including those under the HIPAA. Upon discovery of any such violation by the University or its business associates, the University will promptly investigate the incident and implement appropriate corrective actions. These actions may include notifying affected individuals, retraining employees, enhancing security measures, or taking disciplinary action, as necessary. The University is committed to ensuring that any known harmful effects are mitigated to the extent practicable to protect the privacy and security of individuals' health information.

3. Security

a. General Responsibilities

Any area of campus designated as a University health care component or business associate must comply with all applicable HIPAA security standards, including but not limited to the following:

- Implement reasonable and appropriate procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule in writing either in paper records, or electronically. The documentation must be retained for at least six years from the last date that the document was in effect.

- Comply with the security procedures to assist in providing appropriate administrative, technical and physical safeguards with respect to all ePHI.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and must protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required.
- Develop and implement reasonable and appropriate training related to the HIPAA Security Rule.
- Periodically perform a risk assessment and develop a risk management plan.
- Review periodically, and update as needed, its policy, procedures, and other documentation in response to environmental or operational changes affecting the security of the ePHI.

All University users and units are responsible for the security of information within their control and for complying with all State and Federal Regulations, and University Cybersecurity policies, procedures and guidelines. Application Owners (colleges, departments, or individual users) are responsible for establishing, maintaining, and documenting security controls for all IT systems and data they control. When an application/IT System maintains confidential information subject to regulatory requirements (*e.g.*, HIPAA), the Application Owner will be required to create a written Systems Security Plan (SSP). Typically, documenting a SSP and developing, implementing, and monitoring controls is a collaborative effort by the Office of Information Technology (OIT), Application Owners, Distributed Information Technology units, and for areas falling under the Vice President for Research and Economic Development, the Research Information Systems (RIS) Office.

Additionally, University policy holds users accountable for using IT resources in an ethical and lawful manner, abiding by local, state, and federal law, as well as all other applicable university policies. See the University's Security of IT Resources (06.01.02) policy.

b. Security Risk Assessments

The Departmental HIPAA Privacy Officers shall work with the UAH HIPAA Privacy Officer and the UAH Chief Information Security Officer to conduct and document formal security risk assessments every three (3) years, or as otherwise required by governing regulations or any time there is a material change in the Departmental and/or campus security controls environment.

Security risk assessments shall be done in compliance with the HIPAA Security Rule and shall address administrative, physical, and technical safeguards. Security risk assessments shall use the most current iteration of the HIPAA Security Risk Assessment Tool, available from the HealthIT.gov website. Components of the security risk assessments shall include, but not be limited to:

- Asset inventory;
- Data criticality analysis;
- Threat assessments;
- Determination of risk exposures; and
- Development of a risk mitigation strategy.

c. Annual Security Risk Assessment Review and Updates

Departmental HIPAA Privacy Officers shall review and update security risk assessments at least annually. Documentation of the required annual review shall be maintained by the Departmental HIPAA Privacy Officers, who shall provide annual updates to the University HIPAA Compliance Officer.

The required three-year formal security risk assessment shall count as the required annual review and update for the third year of each assessment cycle.

Data produced from the risk assessments shall be kept confidential. A written record of the analysis/assessment should be maintained by the Departmental HIPAA Privacy Officers for 6 years.

d. Business Associate Requirements

The University requires all business associates to enter into a standard BAA using the University's approved template. This agreement ensures that business associates implement and maintain appropriate safeguards to protect the privacy and security of PHI in accordance with applicable federal and state regulations, including HIPAA. In cases where a business associate cannot use the University's standard template, the agreement must, at a minimum, meet the requirements outlined in the template, including administrative, physical, and technical safeguards to secure PHI and mitigate any potential risks of unauthorized access or disclosure.

4. Breach Notification

a. General Responsibilities

University health care components and business associates must comply with the Breach Notification Rule (45 CFR 164.400-414) and Alabama law, including the Alabama Data Breach Notification Act if there is a breach or any other security incident involving PHI.

To meet that requirement, it is the responsibility of all supervisors and employees to immediately report any breaches to the HIPAA Privacy Officer. Any inadvertent or unauthorized access, use, or disclosure of information will be analyzed to determine when individuals whose information was breached need to be notified.

University health care components must also notify the Office of Compliance and Risk Management (“ORMC”) of any known or suspected breaches without undue delay. The University’s IT Incident Reporting and Breach Notification (06.01.07) provides the processes for documenting IT incident reporting and for notification of Breaches. All breaches shall be reported through this established policy in addition to the required notification to the HIPAA Privacy Officer.

b. Determining if a PHI Breach Occurred

The HIPAA Privacy Officer, along with other institutional officials, will determine if a breach of information has occurred. A breach is, generally, an impermissible use or

disclosure under the HIPAA Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the health care component demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

c. Breach Notification Requirements

The HIPAA Privacy Officer in coordination with appropriate institutional officials must provide notification of a breach of unsecured protected health information to affected individuals, the Secretary of the United States Department of Health & Human Services, and in certain circumstances breaches affecting more than 500 individuals, to the media. Also, business associates must notify the HIPAA Privacy Officer that a breach has occurred.

i. Individual Notice

The HIPAA Privacy Officer must notify affected individuals following the discovery of a breach of unsecured PHI. These individual notifications must be provided without unreasonable delay and in no case later than sixty (60) calendar days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the impacted University health care component. Additionally, a substitute notice provided via HIPAA Privacy Officer Web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the University to determine if their protected health information or personally identifying information was involved in the breach.

ii. Media Notice

Reports of breaches affecting *fewer than five hundred (500)* individuals must be made to the appropriate agency, including the Secretary of the Department of Health and Human Services, no later than sixty (60) calendar days after the end of the calendar year in which the breaches are discovered. In the event the breach affects *five hundred (500) or more* individuals, additional requirements exist, including media notification.

iii. Notice to the Secretary of the United States Department of Health and Human Services

In addition to notifying affected individuals and the media, when appropriate, the HIPAA Privacy Officer must notify the Secretary of the United States Department of Health and Human Services (“Secretary”) of breaches of unsecured protected health information. The HIPAA Privacy Officer will be required to provide this notification by submitting an

electronic breach notification. If a breach affects 500 or more individuals, the University Privacy Officer must notify the Secretary without unreasonable delay and in no case later than sixty (60) calendar days from the discovery of the breach. All notification requirements will be handled by the HIPAA Privacy Officer.

iv. Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify HIPAA Privacy Officer, without unreasonable delay and in no case later than five (5) business days, following the discovery of the breach, unless otherwise provided in an applicable business associate contract. To the extent possible, the business associate should provide HIPAA Privacy Officer with the identification of each individual affected by the breach, as well as any information required to be provided by the University in its notification to affected individuals.

d. Exceptions to Breach Notifications

In accordance with federal regulations, there are some exceptions when an individual(s) does not need to be notified of a breach. However, this determination will be made by the HIPAA Privacy Officer in coordination with the Office of Counsel. The University has the burden of proving why a breach notification was not required and must document why impermissible use or disclosure fell under one of the exceptions.

5. Personnel Designations

All personnel within the University's designated health care components are required to strictly adhere to the HIPAA and all related regulations governing the protection of patient health information. The University is committed to ensuring compliance with HIPAA and has designated specific individuals to provide oversight and supervision of its HIPAA compliance program. These designated individuals are responsible for monitoring adherence to HIPAA standards, providing guidance and training to personnel, and addressing any compliance concerns that may arise to maintain the integrity and confidentiality of PHI.

a. HIPAA Privacy Officer

The University's President shall designate a HIPAA Privacy Officer who is responsible for developing implementing, maintaining, and overseeing the policies and procedures regarding health information privacy to ensure the University continues to comply with the Privacy and Security Rule. In particular, the HIPAA Privacy Officer is primarily responsible for the following:

- Developing and implementing, in collaboration with relevant stakeholders, privacy standards in compliance with the HIPAA Privacy Rule, HIPAA Security Rule, and all other relevant HIPAA regulations and standards.
- Reviewing regular reports regarding personnel training assignments before the expiration of the training window and encourage completion of the requirements.

- Working with Departmental HIPAA Privacy Officers to address any training concerns and remediation follow up for individuals who fail to complete training.
- Overseeing annual risk assessment reviews and updates.
- Collaborating with Departmental HIPAA Privacy Officers to address any needed corrective action(s) and/or mitigation strategies identified during any security risk assessment.
- Performing an institution-level review of all submitted risk assessments to determine enterprise level needs. Work with relevant stakeholders to develop appropriate solutions to meet identified needs.
- Supporting investigations of any reported Breaches.
- Maintaining a log of Breaches reported and submit any needed reports to University leadership or HHS regarding Breaches.
- Reviewing all BAAs in coordination with the University contract management processes for risk assessment and review.
- Developing, maintaining, and making available on the University's website a Notice of Privacy Practices that describes the uses and disclosures of PHI that may be made, the rights of individuals under HIPAA privacy rules, the legal duties with respect to the PHI, and other information as required by the HIPAA privacy rules.

The Privacy Officer will also work with Departmental Privacy Officers from each University designated health care component to communicate and implement this Policy.

b. Departmental Privacy Officers

Each University health care components shall designate Departmental HIPAA Privacy Officers who shall be responsible for coordinating HIPAA Privacy Rule and Security Rule compliance within the University health care component. These designated individuals shall be primarily responsible for the following:

- Verifying department compliance with the requirements of this Policy and certify such compliance to the University HIPAA Privacy Officer, leadership and/or other designated personnel within the department;
- Ensuring all personnel in the covered department (including but not limited to faculty, staff, students, adjunct professors, visiting professors, and volunteers) who are treating patients and/or accessing PHI have been provided at a minimum:
    - Initial HIPAA Privacy Training at the time of their appointment;
    - Annual HIPAA Privacy Training for each year personnel remain affiliated with the Covered Entity; and
    - Additional training on new or revised rules and regulations as required.
- Reviewing routine reports of all personnel who fail to complete any assigned HIPAA Privacy Training. Upon verification of failure to complete training, the Departmental HIPAA Privacy Officer is expected to:
    - Submit a remediation plan for approval with the University HIPAA Privacy Officer for personnel that failed to complete the mandatory HIPAA Privacy Training by the assigned deadline.
    - The remediation plan shall be submitted no later than five (5) business days after expiration of the training window.

    - An approved remediation plan shall be completed by the involved personnel no later than fourteen (14) days after the expiration of the training window.
    - The Departmental HIPAA Privacy Officer will verify compliance with the remediation plan and completion of training to the University HIPAA Privacy Officer.
- Terminating access to all University accounts providing access to PHI, regardless of format, for personnel that fail to complete mandatory HIPAA Privacy Training by the assigned deadline.
- Working with departmental leadership to recommend and implement disciplinary action, up to and including termination for failure to comply with mandatory training.
- Conducting an annual risk assessment review and update, using a HIPAA Security Risk Assessment Tool, and provide a copy to the University HIPAA Privacy Officer.
- Conducting a three-year formal, comprehensive security risk assessment in accordance with the requirements listed in the Security Risk Assessment section above.
- Working with the University HIPAA Privacy Officer to address any corrective action(s) and/or mitigation strategies as identified in the security risk assessments.
- Working with Procurement / Contract Management to verify that all new and renewed BAAs executed for the department contain language that the Business Associate will comply with applicable provisions of HIPAA, and any applicable federal or state regulations regulating PHI.
- Immediately investigating and report all known or suspected Breaches of PHI upon discovery, but in no event later than 24 hours after discovery, in accordance with the UAH IT Incident Reporting and Breach Notification Policy (06.01.07), and notify the University HIPAA Privacy Officer immediately.
- Maintaining a log of all known or suspected Breaches or near misses, and submit that to the University‘s HIPAA Privacy Officer as requested to facilitate required reporting.

6. Training

The University shall train all members of its University health care components’ workforces on the federal HIPAA privacy and security regulations and its HIPAA-related policies and procedures. This training is required for all workforce members of a University health care component. Training should be completed within the first thirty (30) calendar days of employment or assignment and refresher training should be provided on an annual basis thereafter. A procedure will be maintained to follow-up on members of the workforce who are delinquent in completing the required training. Successful completion of this training will be documented.

Documentation of all required HIPAA training, both initial training and annual refresher training as well as other compliance activities will be maintained for at least six (6) years form the date of the implementation.

7. Disciplinary Actions

The University, through its University health care components, shall partner with leaders to apply disciplinary actions against members of the workforce who fail to comply with the University's HIPAA policies and procedures or applicable laws regarding PHI. The Human Resources Department will partner with leaders to implement appropriate, fair, and consistent sanctions for workforce members who fail to comply. They will consider all relevant factors in determining the nature and severity of the disciplinary action, including but not limited to: the type of violation, the intent of the workforce member at the time of the violation, and the number and frequency of any prior violations. Cumulative disciplinary actions may be imposed on an individual who commits more than one violation in one incident.

Employees with access to PHI who fail to comply with HIPAA requirements may be subject to the University's disciplinary policies which can allow for disciplinary action up to and including termination. Students who violate this Policy may face disciplinary action through the Code of Student Conduct. In addition, HIPAA violations may subject an individual to civil and/or criminal penalties imposed by regulatory agencies, civil courts, and/or criminal courts.

Business Associates, vendors, or contractors who are determined by the University to be in violation of HIPAA or University policy may be determined to be in breach of contract and the agreement is then subject to immediate termination. Business Associates who do not follow applicable HIPAA or contractual requirements could be subject to other legal remedies available to the University.

8. Record Retention

Each University health care component will maintain, until six (6) years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the HIPAA Privacy Rule requires to be documented.

9. Intersection with Other Laws and Policies

The handling of student records, including both PHI and PII, is governed by the Family Educational Rights and Privacy Act (FERPA). A student's clinic treatment records from a visit to the University's Student Health Center would be protected under FERPA. In addition, to the extent that those records are transmitted electronically for any billing purpose or other HIPAA-covered activity, HIPAA also applies. For more information on FERPA and student records, see the University's Student Records Policy (03.01.01).

Additionally, as referenced above, the following University policies may be applicable:

- Protection of Data Policy (06.01.01)
- Security of IT Resources (06.01.02)
- Appropriate Use of IT Resources (06.01.03)
- IT Incident Reporting and Breach Notification (06.01.07)
- Student Records Policy (03.01.01)

10. Definitions

While this Policy adopts and incorporates definitions as specified in HIPAA, the same as if fully set forth herein, the following are included for reference:

Breach: An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

Business Associate: A person or entity (other than an employee of a UAH Covered Entity) who performs a function or activity involving the use or disclosure of protected health information, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, for or on behalf of a Covered Entity. *A Business Associate of one UAH Covered Entity does not become a Business Associate of any other UAH Covered Entity simply by virtue of the UAH affiliation.*

Electronic Protected Health Information ("ePHI"): A form of PHI that is transmitted by electronic media or maintained in electronic media.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, (including amendments) that establishes standards to safeguard the PHI held by Covered Entities or their Business Associates.

Protected Health Information ("PHI"): Individually identifiable health information that is collected from an individual, created or received by a health care provider, health plan, health care clearinghouse, or other employee of one of the Covered Entities or Business Associates of the University. PHI includes, but is not limited to information regarding:

- the individual's past, present or future physical or mental health or condition;
- the provision of health care to the individual; or
- the past, present, or future payment for the provision of health care to the individual; and
- that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
- Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number, phone numbers, photographs, medical record numbers, account numbers, employer, or any other identifying information that could reasonably be used to determine the identity of a person).

11. Review

The Office of Risk Management and Compliance shall review this policy every five (5) years or sooner if circumstances warrant.