- x UAH Office of Risk Management and Compliance
- x UAH Office of Information Technology
- x UAH Payroll Services
- x UAH Human Resources
- x Other University units or departments to the extent that their activities are subject to Business Associate Agreements ("BAA")
- x Other University units or departments to the extent that they access and/or create PHI for research purposes
- x 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

- *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

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(u)bNge.3 (r)4.9 (t)-6.6 (i)2inoons muz(i)2.6 (f)-6.(ov)8.9 (e1nf)-17.o6ec 0 Tc 00.5 (e e

- *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

t2 Ave (U)2.6 (po)10.5es-6.6 ( )2.6 (c)-2 (e)10.5 (ton)

- 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

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 breamust

    - 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

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