1. Title

Breach Notification Policy

2. Policy

Sec. 1 Policy Statement. The Health Insurance Portability & Accountability Act (HIPAA) & HITECH Acts and implementing regulations require Covered Entities and their Business Associates to investigate and mitigate any security or other incidents that involve potential unauthorized access of Protected Health Information (PHI) as that term is defined by HIPAA. Except in very limited instances, any unauthorized access to a Covered Entity's PHI constitutes a breach. Breaches that impact fewer than 500 individuals must be reported to impacted individuals within 60 days of discovery and reported on an annual basis to Health and Human Services (HHS). Breaches that impact 500 or more individuals must be reported to HHS, the media, and the impacted individuals within 60 days of discovery.

Additionally, Texas Government Code Section 2054.1125 clarifies that the breach reporting statutes in Business & Commerce Code Section 521.053 apply to state agencies and institutions of higher education persons. Notices of breaches involving unencrypted Sensitive Personal Data maintained in or obtained from a computerized data base must be provided by such entities to all affected individuals.

System Administration is a Covered Entity required to comply with HIPAA and also maintains Sensitive Personal Data in many of its offices and departments. It is the Policy of System Administration to comply with HIPAA and or Texas Government Code Section 2054.1125 at all times. This Policy describes how System Administration will comply with its Breach notification duties under HIPAA and or Texas Government Code Section 2054.1125. It applies to all U. T. System Administration Workforce Members.

Sec. 2 Duty to Report to System Officials.

2.1 Reporting Potential Breaches Involving PHI. All Workforce Members are required to report to the Privacy Officer, within 24 hours of discovery, any possible Incident of inadvertent disclosure or unauthorized access of PHI that may constitute a Breach. Reports made after business hours can be made via email to Privacyofficer@utsystem.edu.

2.2 Reporting Potential Breaches Involving Electronic Data. All security Incidents that involve System Administration Electronic Information Security Resources, including data, that may involve Sensitive Personal Data or PHI (collectively Protected Data) should be reported to the System Administration Information Security Officer who shall relay such reports to the Systemwide Information Security Officer (ISO). All such reports received by the ISO shall be reported immediately to the HIPAA Privacy Officer by the ISO, or in the absence of the ISO, the ISO's designee. This report must be made in addition to any reporting required in the System Administration's information security polices or other applicable policies.

2.3 Reporting by Contractors. All Contracts and Agreements of any kind, including Business Associate Agreements, that involve access or use of System Administration Protected Data, shall require the contractor to notify a designated System Administration official of any unauthorized use or disclosure by the Contractor or its workforce, agents, or subcontractors that constitutes a security Incident involving Protected Data and the remedial action taken or proposed to be taken with respect to the use or disclosure. Any official receiving such a report must immediately forward any such report pertaining to the potential access of electronic Protected Data to both the HIPAA Privacy and Security Officers. All reports of inappropriate uses or disclosures of Protected Data from a non-electronic source must be immediately forwarded to the HIPAA Privacy Officer.

2.4 Reporting to the Chancellor. The ISO shall notify the Chancellor without delay of any reported security Incident involving Protected Data in electronic form that, upon preliminary investigation, could constitute a Breach. The Privacy Officer shall notify the Chancellor without delay of all other unauthorized use or access of PHI that could constitute a Breach.

2.5 Reporting Processes. Each office or department within System Administration shall require its Workforce Members to immediately report any Incident, upon Discovery, to the Privacy Officer or System Administration's Information Security Officer, as applicable, in accordance with this Policy. Offices and Departments shall not conduct internal investigations prior to, or otherwise delay, timely notification of the Privacy Officer or System Administration's Information Security Officer. The

Policy must require a reporter to error on the side of caution and report an Incident when determining whether to make a report or not.

Sec. 3. Breach Response Team; Duties

3.1 Breach Response Team. A Breach Response Team shall be assembled to investigate and determine System Administration's compliance duties as to each Incident reported to the Chancellor as a security Incident or unauthorized use or access of PHI that could trigger System Administration's duty to provide breach notifications under applicable federal or state privacy laws.

(a) Members. The Privacy Officer, or both the Privacy Officer and the ISO if the Incident involves access to PHI through an electronic information resource, will work with any other System official or the official's designee, who, based on the nature of the incident, is deemed to have experience or skills that make them appropriate for inclusion as a members of a Breach Response Team. Such other individuals may include, but are not limited to: the Chief Information Officer, the Director of Employee Benefits, the Vice Chancellor for Public Affairs, the General Counsel, and the Director of Employee Services. The team may also include the director or Workforce Members of the office or department that is the owner of the affected Protected Data, provided that inclusion of such individuals does not present a conflict of interest. The Privacy Officer and/or the ISO shall act as the directors or co-directors of the System Administration's investigation of and response to the Incident.

(b) Duties. The duties of the Breach Response Team shall include, at a minimum, as applicable:

(i) ensuring that all appropriate actions are immediately taken to prevent any further unauthorized exposure of Protected Data;

(ii) investigation of the Incident, which may include interviewing relevant Workforce Members to learn about circumstances surrounding the incident and/or reviewing logs, tapes, and/or other resources;

(iii) identifying and engaging non-System Administration consultants, as required to assist the System Administration in its investigation and/or risk analysis;

(iv) conducting a risk analysis to determine whether a Breach has occurred;

(v) conducting a root cause analysis of the Incident;

(vi) developing a mitigation plan to prevent any further exposure of Protected Data and/or risk of harm to anyone affected by the Breach, which may include revision of the System Administration's Policies and/or additional workforce training;

(vii) determining the appropriate notification requirements required and developing an action plan for the delivery of such notices;

(viii) if the Incident involves any violations of the System Administration's Privacy Policies by a member of the HIPAA workforce, referral of the Workforce Member(s) to the Privacy Officer for appropriate actions, including sanctions in accordance with Policy INT166 of the System Administration Privacy Manual;

(ix) if the Incident involves a Business Associate or its subcontractor or other contractor, recommending termination or amendment of the terms of the Business Associate Agreement or other contract if required;

(x) compliance at all times with applicable legal and regulatory requirements;

(xi) keeping the Chancellor informed of the progress of the team; and

(xii) oversight of the content and distribution of all internal communications, and in collaboration with the Office of Public Affairs as applicable, external communications about the Incident, including Breach notifications.

3.2 Law Enforcement. At any time during the process, upon determination by the Privacy Officer or the Chief Information Security Officer that it is likely that the Incident may be the result of criminal action, or if for any other reason, the team determines that law enforcement participation is required or advisable, System Administration police, local law enforcement agencies, and/or the FBI, as appropriate, shall be notified without delay.

Sec 4. Individual and Other Required Notifications.

4.1 Notification of Individuals:

(a) Timing. Upon determining that a Breach has occurred, System Administration (or in some cases, if the Breach involves a Business Associate, the Business Associate) will make the individual notifications as soon as reasonably possible after the covered entity takes a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual but in no case shall notifications take place later than 60 days following the discovery of a breach, except when an agency of law enforcement requests a delay. Any delay based on law enforcement request must be documented in writing provided by or acknowledged in writing by the requesting law enforcement authority enforcement. System Administration may provide the required information as part of the notification process to individuals within the required time period in multiple mailings as the information becomes available.

(b) Process. Unless otherwise determined by the Chancellor, the System Administration office or department with responsibility for the Protected Data that was the subject of the Incident will be responsible for working with the Privacy Officer and the Office of Public Affairs to ensure that the required reporting to individuals and media occurs. All notices including substitute and media notices when applicable shall contain the following, 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 which shall include a toll free number where recipients can receive information and get answers to their questions about the breach.

(c) Business Associates. In the case of a Breach involving a Business Associate, notifications may be handled by System Administration or the Business Associate, as determined by the System Administration, depending on the terms of the Business Associate Agreement in place and the circumstances surrounding the incident.

4.2 Reports to HHS will be made by the Privacy Officer.

4.3 Reports to the media shall be made by the Office of Public Affairs in consultation with the Privacy Officer.

4.4 Reports required by other laws will be made by the Privacy Officer in consultation with the Vice Chancellor and General Counsel.

4.5 System Administration's Offices of the Chancellor and Public Affairs shall receive advance notice prior to the notification of any affected individuals, the System Administration community, the media, or HHS sufficient to enable those offices to prepare to respond effectively to inquiries regarding the Breach.

3. Definitions

Breach - any unauthorized access or use or other exposure of an individual's Protected Data that triggers a duty under state or federal law to provide a notification to the individual or a third party.

Business Associate - Any entity that contracts with a Covered Entity to provide services that require the entity to access, use, maintain or disclose the Covered Entity's PHI.

Covered Entity - A health care provider, health plan or clearinghouse that is required to comply with HIPAA.

Discovered, Discovery - A Breach shall be treated as discovered by University, or a contractor, including a Business Associate or the contractors' subcontractor, as of the first day on which an Incident that is subsequently determined to be a Breach is known or should reasonably have been known to the University,

contractor, or subcontractor, as applicable, even if it is initially unclear whether the Incident constitutes a Breach.

HIPAA - Health Insurance Portability and Accountability Act (HIPAA) as specifically set forth in Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 as the Administrative Simplification provisions and the regulations adopted by the U.S. Department of Health and Human Services (HHS) to implement HIPAA which give HHS the authority to establish standards and requirements for the electronic transfer of health care information, and for the privacy and security of PHI.

Incident - Any unauthorized use, disclosure, or event that could reasonably involve Protected Data and/or indicates that a Breach has occurred.

Protected Health Information (PHI) - Individually identifiable health information that is transmitted or maintained in any medium or form that is subject to HIPAA. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended; in records described at 20 U.S.C. §1232g(a)(4)(B)(iv) (student treatment records excepted from FERPA); and in employment records held by a covered entity in its role as an employer.

Protected Data - Information maintained by or for System Administration offices that is subject to the Breach notification requirements of HIPAA/HITECH and/or Texas Business & Commerce Code Chapter 523 or other state or federal breach notification.

Sensitive Personal Data - information stored in or derived from an electronic data base that includes: (i) an individual's last and first name or initial plus a Social Security Number, Driver's License or other state issued ID number, or account information plus a PIN or password; or (i) information that identifies an individual and relates to the individual's physical or mental condition, or the provision of health care to, or payment of healthcare for, the individual.

Workforce Members - Officers, employees, volunteers or any other individual or contractors who provide services or conduct business on behalf of The University of Texas System.

4. Relevant Federal and State Statutes

Health Insurance Portability and Accountability Act (HIPAA)

Texas Business & Commerce Code Chapter 523, Provisions Relating to Victims of Identity Theft

Texas Government Code Section 2054.1125, Information Resources, Security Breach Notification by State Agency

5. Relevant System Policies, Procedures, and Forms

INT166, System Administration Privacy Manual

UTS165, Information Use & Security Policy

6. System Administration Office Responsible for Policy

Office of General Counsel

7. Dates Approved or Amended

September 23, 2013

Revised January 20, 2017