**Overview on HIPAA Compliance at The University of Texas System**

Barbara Holthaus

Assistant General Counsel& System-wide Privacy Coordinator

Office of General Counsel

The University of Texas System

September 8, 2015

HIPPA commonly refers to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by The Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act (ARRA) of 2009, and regulations, issued by the U.S. Department of Health and Human Services (HHS). HIPAA protects the privacy and security of individual health information used, transmitted, and retained for the provision and payment of health care services. This information is known as protected health information (PHI).

PHI includes virtually any information from an individual’s medical records, records of payment for medical services made by or on behalf of a person (including insurance claims and reimbursements), or information provided to a health care provider about an individual’s physical or mental health or condition that identifies or can be used to identify the individual.[[1]](#footnote-1)

Typically, employment records and student education records that contain health information or information about payment for health services about an individual, as well as student treatment records from System institution’s student health center or counseling centers, are exempt from HIPAA. However, health and health payment records contained in an employment record held by a UT System institution are subject to state privacy laws. Student education records are protected by another federal privacy law, the Family Educational Records Privacy Act (FERPA), while student treatment records are regulated by state medical confidentiality laws.

HIPAA applies to all health insurance plans and health care billing clearinghouses, and to health care providers (such as hospitals, physicians, and clinics) that bill insurers electronically. These entities are collective called “HIPAA Covered Entities”. HIPAA also applies to third parties such as attorneys, information technology service providers, auditors, and other service providers (“Business Associates”) who access a Covered Entity’s PHI in order to provide services.

HHS implements HIPAA and enforces HIPAA through its Office of Civil Rights. Civil violations are punishable by penalties that can run from a minimum of $100 to $50,000 per day of violation, with an annual cap of $1.5 million for the same violation in any one year. Criminal penalties can also be imposed that are applicable to individuals for violations. In cases of “knowing misuse,” criminal penalties include monetary fines of $50,000 up to $250,000, and imprisonment of one (1) to ten (10) years.

**THE HIPAA REGULATIONS**

There are three main sets of HIPAA regulations that apply to Covered Entities and Business Associates:

**The Privacy Rule** requires Covered Entities and Business Associate to adopt appropriate safeguards to protect the privacy of personal health information (PHI), including individual medical records; and, set limits and conditions on the uses and disclosures that may be made of such information. The Privacy Rule also gives individuals rights over their health information, including the right to examine and obtain a copy of their health records, and to request corrections. In general, unless the individual has provided written consent (called an “Authorization”), an individual’s PHI can only be accessed by a member of the workforce of a Covered Entity or Business Associate for treatment or payment purposes or to perform specific health care operations. PHI can only be released to third parties outside the Covered Entity or Business Associate under specific exceptions permitted by the Privacy Rule. Examples of these exceptions include disclosures and access: required to defend the Covered Entity in a legal action brought by a patient of the Covered Entity; required by law, or for health and safety or law enforcement purposes; pursuant to a valid subpoena or court order; or, to prevent potential harm to the individual or others.

**The Security Rule** requires the implementation of physical, administrative and technological safeguards to ensure confidentiality and data integrity of electronic PHI, and to prevent unauthorized use of and guard against physical hazards to electronic PHI. The Security Rule requires Covered Entities and Business Associates to:

• Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

• Identify and protect against reasonably anticipated threats to the security or integrity of the information;

• Protect against reasonably anticipated, impermissible uses or disclosures; and

• Ensure compliance by employees, officers and volunteers who are part of the Covered Entity or Business Associate’s workforce.

**The Breach Rule** requires Covered Entities and their Business Associates to investigate and mitigate any security or other incidents that involve potential unauthorized access to, or use or disclosure of, PHI. 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 HHS. Breaches that impact 500 or more individuals must be reported to HHS, the media, and the impacted individuals within 60 days of discovery.

**HOW HIPAA COMPLIANCE WORKS AT UT SYSTEM**

Due to the diversity of the missions of the nine academic institutions, the six health science centers, and the offices that comprise UT System Administration, UT System does not operate as a single entity for HIPAA compliance purposes.

The following institutions are not subject to HIPAA at all: The University of Texas at San Antonio, The University of Texas at Arlington, The University of Texas at El Paso, and The University of Texas at Tyler. None of these institutions currently engage in any health care operations that are subject to HIPAA or create of maintain PHI. The University of Texas of the Permian Basin serves as the Business Associate of another state agency that is a HIPAA Covered Entity and has compliance duties limited to the PHI it accesses on behalf of that Covered Entity.

The University of Texas at Arlington at one point provided services that required it to comply with HIPAA, but no longer does so. Therefore, it has some remaining compliance duties as to records that are subject to HIPAA and still being held by the University under record retention requirements, but it has no active HIPAA compliance duties.

All of the six health science institutions- The University of Texas MD Anderson Cancer Center, The University of Texas Medical Branch Galveston, The University of Texas Southwest Medical Center, The University of Texas Health Science Center Houston, The University of Texas Health Science Center San Antonio, and The University of Texas Health Science Center Tyler are HIPAA Covered Entities. Each of them provides health care services that involve the creation and maintenance of PHI through the operations of hospitals, physicians’ practice plans, and/or the provision of other health care related services that is subject to HIPAA.

UT System Administration[[2]](#footnote-2), UT Austin[[3]](#footnote-3), and UT Dallas[[4]](#footnote-4) are each designated as a Hybrid Entity under HIPAA.  UT Rio Grande Valley has not yet designated a HIPAA Covered Entity, but will most likely be a Hybrid Entity, as well. This means that some of their offices are required to comply with HIPAA and some are not. Offices within a Hybrid Entity that access PHI must be designated as the Hybrid Entity’s “Health Care Component. PHI can be shared freely within the Health Care Component to perform health care related business functions. However, PHI cannot be shared outside of these offices, even with other offices at the same institution, absent a signed an authorization consenting to the release or under specific exceptions permitted by HIPAA.

Each of the Covered or Hybrid Entity within System are individually and directly subject to the jurisdiction of HHS. Each has its own separate HIPAA compliance programs and policies that reflect the institutions unique configurations its own HIPAA Privacy and Security Officers.

Because each UT System institution subject to HIPAA is a separate legal entity, PHI cannot be shared among any of the institutions or with System Administration offices absent a signed authorization from the patient or an applicable exception within the Privacy Rules that would permit it to be disclosed.[[5]](#footnote-5) Information that has been de-identified to remove all potential identifiers is not considered to be PHI and can also disclosed and used generally without restriction.

Some offices within System Administration, such as the Office of General Counsel,[[6]](#footnote-6) are required to provide services to System Institutions that are Covered Entities. These offices can access these institutions’ PHI under the HIPAA “Business Associate” exception. This exception allows a person or entity that provides services to a Covered Entity to access the Covered Entity’s PHI, but only for the purpose of providing the services. The Business Associate must have a HIPAA compliant Business Associate Agreement or MOU with the Covered Entity and cannot share the PHI it accesses under the Agreement internally outside of its Health Care Component or with outside parties, except as expressly permitted by the Business Associate Agreement or MOU, or as otherwise permitted by HIPAA. Business Associates, including the System Administration offices that access PHI from System institutions, are directly subject to HIPAA and are subject to investigation, audits and enforcement actions and penalties to the same extent as Covered Entities.

In general, PHI released pursuant to a valid authorization, or because it has been de-identified, is no longer subject to HIPAA. However, information disclosed or accessed pursuant to a HIPAA exception or under the terms of certain authorizations may continue to be subject to other state privacy laws that protect the confidentiality of such information. This means that System Administration office that is are not part of the Health Care Component at System Administration, such as the Offices of the Board, the Chancellor, Student Affairs or Health Affairs must exercise caution as to any documents containing PHI that it has accessed under an exception or pursuant to an authorization.

**UT SYSTEM HIPAA Privacy Contacts**

Each institution that is subject to HIPAA, including UT System Administration has a HIPAA Privacy Officer and its own HIPAA Privacy, Security and Breach Notification policies. System Administration’s Privacy Policies, which include its Breach Notification Policy can be found at <http://www.utsystem.edu/benefits/hipaa/> and through a link on the Systemwide Policy Library which is at <http://www.utsystem.edu/bor/procedures/policy/> . Barbara Holthaus, Senior Attorney and Systemwide Privacy Coordinator, Office of General Counsel is the UT System Administration HIPAA Privacy Officer. Her direct line is 512 499 4617 and her email is bholthaus@utsystem.edu. A separate email, Privacyofficer@utsysem.edu is maintained for receiving HIPAA complaints, breach and violation reports. Ms. Holthaus or the Systemwide Compliance Office, <https://www.utsystem.edu/compliance/> can provide contact information for the HIPAA Privacy Officers at System institutions that are subject to HIPAA.

**UT SYSTEM Security Contacts**

Each institution has a designated Information Security Officer (ISO). At institutions that are Covered Entities, the ISO is also the HIPAA Security Officer. Ed Mattison serves as the Systemwide Chief Security Officer. The Office of Systemwide Information Security can provide contact information for each institution’s Information Security Officers. That office can be reached at 512 499-4389. Mr. Mattison’s email is mmattison@utsystem.edu.

**ADDITIONAL RESOURCES**

An excellent source of information on all things HIPAA as well as links to the HIPAA and HITECH Acts and Regulations can be found at:

 <http://www.bricker.com/services/resource-details.aspx?resourceid=217>

Information from the Department of Human Services on HIPAA can be found at:

<http://www.hhs.gov/ocr/privacy/index.html>

1. HIPAA defines PHI as any health information that is created, received, or maintained by a HIPAA covered entity whether in print, orally or electronically, that: 1) includes “individual identifiers” that clearly identify an individual (or has components that could be used to identify the individual); and 2) is related to a past, present, or future physical or mental health condition, or the provision of, or payment for health care or genetic information. [↑](#footnote-ref-1)
2. The offices within the System Administration’s HIPAA Health Care Component are the Office of Employee Benefits (OEB), which houses the UT System’s group employee self-funded medical health plan (UT SELECT), dental plan (UT DENTAL SELECT) and flexible medical savings plan (UT FLEX) which constitute a HIPAA Covered Entity; plus, the Office of General Counsel, which provides health care operations in the form of legal services to the UT System health plans as well as services as the Business Associate of the UT System institutions that are subject to HIPAA; Systemwide Compliance; the Audit Office; the Office of Employee Services; the Office of Technology Services. [↑](#footnote-ref-2)
3. UT Austin has a health center that provides some services to non-students and a Pharmacy School as well as a few other offices that engage in services that are subject to HIPAA. When the new medical school opens, that too will be subject to HIPAA. [↑](#footnote-ref-3)
4. UT Dallas houses the Callier Communication Center for Speech Communication and Hearing Disorders which is subject to HIPAA. Some of its administrative offices provide Business Associate services to the Center which require access to the Center’s PHI. [↑](#footnote-ref-4)
5. There are also state medical and mental health privacy laws that would prevent a hospital or health care provider from sharing identifiable patients records without consent absent the existence of an applicable exception. [↑](#footnote-ref-5)
6. See footnote 3 for a full list. [↑](#footnote-ref-6)