UTHealth
The University of Texas
Health Science Center at Houston

17-201 HITECH Act

We have completed our audit of the HITECH Act. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g. creation of a national health care infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

Because this legislation anticipated a massive expansion in the exchange of electronic protected health information (PHI), the HITECH Act widened the scope of privacy and security protections available under The Health Insurance Portability and Accountability Act of 1996 (HIPAA), increased potential legal liability for non-compliance, and provided for more enforcement.

Under the HITECH Act, business associates are now required to comply with the safeguards contained in the HIPAA Security Rule. Written contracts (Business Associate Agreements) are required from business associates who maintain, create, receive, or transmit PHI for covered entities.

OBJECTIVES

The objective of this audit was to determine compliance with selected requirements of the HITECH Act.

SCOPE PERIOD

The scope period included all applications containing PHI as of October, 2016.

METHODOLOGY

The following procedures were performed:

- Verified policies and procedures pertaining to the execution of Business Associate Agreements (BAAs) exist and are reviewed by the Privacy Officer as needed.
- Reviewed UTHealth's BAA template (Template) and confirmed all provisions required by HIPAA §164.504(e) are included.
- Selected a sample of applications containing PHI, obtained access listings for each application, and identified user accounts associated with vendors/contractors. Selected a sample of the identified vendors/contractors and verified that an executed BAA (using the Template) was in place. For BAAs executed prior to the introduction of the Template, verified HIPAA-required provisions were included.

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

AUDIT RESULTS

A&AS identified areas of improvement related to executing and retaining BAAs, Template guidance, and user access:

- Executed BAAs were not in place for five vendors (four identified by A&AS and one identified by management after further analysis) with access to PHI. A&AS obtained evidence BAAs were subsequently executed with four of the five vendors and verified new processes were implemented to ensure BAAs are executed with vendors before they are allowed to access PHI.
- The Template was not used for 17 BAAs executed after guidance was issued by the Office of Legal Affairs (OLA). A&AS obtained evidence that OLA confirmed with Procurement and UTP that the Template will be used for execution of BAAs (where applicable) going forward. Additionally, A&AS verified OLA approval is now obtained and documented prior to the execution of BAAs that deviate from the Template.
- 33 vendors, contractors, or ex-employees maintained access to one or more selected applications (containing PHI) after termination. A&AS verified access was subsequently removed and a process developed to ensure users no longer have access to applications after termination.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None.

We would like to thank the staff and management within the School of Nursing, School of Dentistry, Harris County Psychiatric Center, McGovern Medical School, Office of Legal Affairs, Procurement, Administrative Technology, and Clinical Technology who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

MAPPING TO FY 2017 RISK ASSESSMENT

Risk (Rating)	R.1 A BAA has not been executed with each vendor who accesses PHI (High)

DATA ANALYTICS UTILIZED

Data Analytic #1	Using data analytics software, compared access listings to the UTHealth directory to confirm user affiliation and job title.

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA

Auditor Assigned	Brittney Alexander
End of Fieldwork Date	June 9, 2017
Issue Date	June 14, 2017

Copies to:
Audit Committee
Richard Miller
Melissa Pifko
Andrew Casas
Dr. James Griffiths
Dr. Kimberly Ruona
Dr. Muhammad Walji
Stephen Glazier
Kristi Bradley
Bassel Choucair
Kristine Estes
Christina Solis

Issue #1	The HITECH Act requires business associates to comply with the safeguards contained in the HIPAA Security Rule. *HIPAA Security Rule 164.308* states that written contracts are required from business associates who maintain, create, receive or transmit PHI for covered entities. The business associate is required to safeguard this information according to the HIPAA Security Rule. A&AS obtained the critical application inventory listing and inquired with schools/areas across UTHealth about other applications containing PHI. We judgmentally selected a sample of 23 applications containing PHI and reviewed access listings to confirm if vendors/contractors had been granted access. For each application in our sample, we selected a sample of vendors/contractors and obtained executed BAAs. We noted executed BAAs were not in place for five vendors (four identified by A&AS and one identified by management after further analysis) with access to PHI. A&AS verified BAAs were subsequently executed with four of the five vendors and new processes were implemented to ensure BAAs are executed with vendors before they are allowed to access PHI. For the remaining vendor, an analysis is being performed to determine if a BAA is applicable based on the services provided.
Recommendation #1	We recommend SoD work with the Office of Legal Affairs to identify whether a BAA is necessary based on the services provided by the vendor. If it is determined a BAA is required, we further recommend SoD and Legal Affairs work with the vendor to obtain a BAA.
Rating	Medium

Management Response 1	As the Simplant application is user-friendly, economical, and the preferred choice of our leading clinicians across several departments, retaining the application is our primary objective. SoD personnel in key leadership positions have attempted multiple different avenues to secure a BAA for the Simplant application from the vendor (Dentsply Sirona) and will continue to do so. In the meantime, we are completing a full security assessment of Dentsply Sirona under the direction of Beverly Moore in IT Security. In the event that this issue cannot be resolved, we will assess competing applications suitable for SoD graduate clinics and faculty practices for both 3D-guided implant treatment planning and fabrication of surgical guides and determine the best path forward.
Responsible Party	Dr. Kimberly Ruona, Associate Dean for Patient Care
Implementation Date	July 20, 2017