Serving Harris, Galveston, Brazoria, Fort Bend and Montgomery Counties

Houston Medical Times

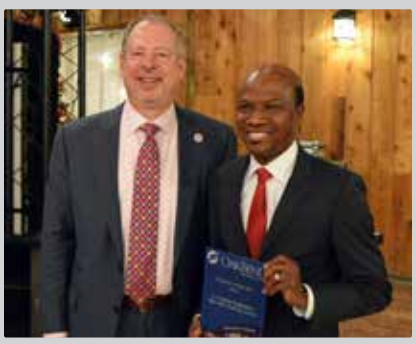
Bringing Healthcare News to the Forefront

Volume 9 | Issue 2 February 2019

Inside This Issue

A Trauma Surgeon's Plea to Houston Drivers
See pg. 9

INDEX



Oakbend Medical Center Announces 2018 Physician Of The Year
See pg. 12

Deal Breaker – Cyber Security Risk in Health Care Transactions

By Iliana L. Peters, J.D.
Lidia M. Niecko-Najjum, J.D.
Polsinelli, PC

Health care organizations' lack of compliance with the data privacy and security requirements of both state laws and the Health Insurance Portability and Accountability Act ("HIPAA") Privacy, Security and Breach Notification Rules and the resulting cyber security risk could be a literal "deal breaker" for mergers and acquisitions. Buyers must prioritize fulsome due diligence in investigating the data privacy and security practices of their targets, and sellers must be prepared to provide excellent documentation regarding their policies and practices to buyers to ensure that the deal does not stall, or worse, based on concerns about potential state and federal regulatory enforcement actions.

Recent business deals in other industries have been affected by cyber attacks, causing a lowered purchase price or resulting in buyers acquiring big liabilities related to previous information breaches. In health care, buyers must also consider state privacy and security laws, and particularly the HIPAA Rules.

Generally, most health care organizations must ensure they are compliant with:

- The HIPAA Privacy Rule which requires the permitted uses and disclosures of Protected Health Information (PHI) and individuals rights to it.
- The HIPAA Security Rule which requires the necessary physical, administrative and technical safeguards that must be put in place to protect confidentiality, integrity, and availability of PHI.
- The HIPAA Breach Notification Rule which requires parties to be notified when a breach of PHI has occurred.

Violations of HIPAA have serious consequences. These include civil penalties that range from $50,000 per incident up to $1.5 million per incident for violations that are not corrected, per calendar year. "Per violation" means that any particular investigation of a breach incident could result in $1.5 million in penalties for each year of a six-year statute of limitations for each requirement of the Privacy, Security or Breach Notification Rules that may be implicated. Both the Department of Health and Human Services (HHS) and the State Attorneys General have jurisdiction to enforce civil penalties. HIPAA violations may also result in criminal penalties that end in more fines and violators facing up to 10 years in prison; the Department of Justice (DOJ) enforces the criminal provisions of HIPAA.

Too many potential buyers do not conduct the requisite HIPAA compliance due diligence and expose themselves both to HIPAA penalties and general cybersecurity liability. At the same time, many sellers do not anticipate that buyers will inquire about HIPAA compliance and are unable to provide key information that should be necessary to complete the deal.

To avoid HIPAA liabilities and cybersecurity risk, due diligence should include a review of the following:

1. Copies of HIPAA Policies and Procedures for the previous six years:

Privacy Rule

- Updated policies and procedures regarding uses, disclosures, and safeguards to protect PHI
- Updated policies and procedures regarding individual's rights
- Updated policies and procedures regarding Business Associate Agreements and sample forms
- Designation of HIPAA Privacy Officer
- Notices of Privacy Practices
- HIPAA Authorization Forms

see Cyber Security... page 14

Cyber Security
Continued from page 1

Security Rule

- Copies of required enterprise Risk Analyses and Risk Management Plans (these are not security audits or gap analyses, for example). Roughly 80% of HHS's settlement agreements and civil money penalties include violations of these requirements
- Updated policies and procedures regarding administrative, physical and technical controls
- Designation of HIPAA Security Officer
- Evidence of technical safeguards required by the HIPAA Security Rule, including encryption, malware protection, access and audit controls, device and media controls, and facility access controls

Breach Notification

- Updated policies and procedures regarding investigating suspected or actual breach incidents and providing notice
- Updated policies and procedures regarding record retention and destruction
- Updated policies and procedures regarding training of employees

2. List of Business Associates and confirmation of existing BAAs
3. Documentation regarding any data security incidents or security breaches, and any open HHS investigations
4. List of complaints received related to HIPAA, and any open HHS investigations
5. Documentation of current Cyber liability insurance

Buyers should consider that reoccurring HIPAA compliance issues found at health care organizations include failure to manage identified cybersecurity risk and insider threats, lack of encryption, lack of appropriate access controls, lack of mobile device controls, improper disposal of PHI, insufficient data backup and contingency planning. Entities also fail to obtain requisite business associate agreements, conduct risk analyses, ensure information transmission security, conduct appropriate auditing and patch their software. These failures, if investigated by HHS, State Attorneys General or the DOJ, would be a real eye opener for potential buyers, maybe even "deal breakers."◆

Oncology
Continued from page 5

5. It's in Your Blood

In 2019, we expect to hear more about advancements in a variety of blood tests as a new approach to detect and diagnosing cancer. Though still in the trial/study phase, recently developed blood tests are being used to detect cancer cells in the bloodstream. As for using blood testing as a wide-spread method of testing for cancer, it's still very early, but developments in this area hold great promise.

As we look to the future, new developments in cancer detection and treatment are exciting. These trends represent advancements that will continue to pave the way forward, leading to better outcomes and quality of life for patients during and after treatment, and ultimately delivering greater hope to everyone impacted by cancer.

Muffaddal Morkas, MD is a Medical Oncologist at Texas Oncology–Memorial City, Houston, Texas. For more information, visit TexasOncology.com. .◆

UT Health
Continued from page 6

have flexible walls that transform them into an auditorium for large-scale events, including conferences and seminars. Technological advances include a modern media lab, which will play host to educational videos and lectures distributed to internal audiences as well as other universities across the country. The new home also offers plenty of space for convenience while studying, including a coffee bar and café area, break room, and cushioned benches.

"We wanted to provide a space for students to feel like they could comfortably spend the day here surrounded by all the resources they would need to succeed in their studies, including access to our faculty and staff," said Amy Franklin, PhD, associate professor and assistant dean at the school.

The 44,709-square-foot facility spans two floors adjacent to UTHealth's University Center Tower (UCT), a size equal to three existing floors. The wider footprint allowed designers to create a more efficient space complete with 230 workstations. The addition sits above the UCT parking garage.

"Constructing a new expanded space on top of a 1970s parking garage came with unique challenges, like ensuring alignment and structural stability, but also distinct financial advantages over trying to construct a stand-alone building," said Ginger Williams, senior project manager. "Our project team worked with others across the university to mitigate the potential risks by separating the project into phases and bringing the general contractor on board to review precision alignment with the existing structure."

This multi-phase process allowed the team to deliver the project at the highest quality, faster than anticipated, and under budget, said Julie Lucas, director of project management.

In 2019, UTHealth School of Biomedical Informatics will launch the first-ever applied Doctorate in Health Informatics program, in addition to its existing PhD program, master's program with two tracks, graduate certificate programs, and dual MD/MS, PhD/MPH, and MS/MPH programs. For more information about the school, its degree offerings, and facilities, please visit UTHealth School of Biomedical Informatics.◆

Houston Medical Times
Bringing Healthcare News to the Forefront

Published by Texas Healthcare Media Group Inc.

Director of Media Sales
Richard W DeLaRosa

Senior Designer
Jamie Farquhar-Rizzo

Web Development
Lorenzo Morales

Distribution
Robert Cox

Accounting
Liz Thachar

Office: 713-885-3808
Fax: 281-316-9403

For Advertising
advertising@medicaltimesnews.com

Editor
editor@medicaltimesnews.com

Houston Medical Times is Published by Texas Healthcare Media Group, Inc. Houston Medical Times is published every month

P.O. Box 57430

Webster, TX 77598-7430