About the Speaker
Richard Y. Cheng

Richard Y. Cheng is a Member at Dykema Cox Smith, based out of their Dallas office. His practice is focused on representing health care providers involving corporate transactions, government audits, medical appeals, regulatory and compliance matters. Specifically, Richard regularly advises health providers on issues involving Stark, Anti-kickback, OIG provider self-disclosures, HIPAA, HITECH Act, corporate integrity agreements (CIAs), acquisitions, divestitures, joint ventures, CMS related violations, state agency violations and other healthcare operational matters. In addition, Richard has extensive knowledge with representing clients before administrative law judges with the Office of Medicare Hearings and Appeals and Departmental Appeals Board, Civil Remedies Division.

Richard was selected by his peers as a *D Magazine* "Best Lawyer" in health care and as a *Thomson Reuters* Texas "Rising Star." Also, Richard won the 2011 *Dallas Business Journal* "Best Corporate Counsel Rising Star" award, was recognized twice as a finalist for the *D CEO Magazine*/ACC best corporate counsel award, was awarded the National Diversity Council Legal Diversity Champion Award in 2012, received the 2011 and 2012 TOTA Distinguished Service awards and was recognized by Texas Tech University HSC as a 2010 Distinguished Alumni.

Prior to his legal career, Richard worked as a licensed occupational therapist in Dallas, Texas. He has served as an adjunct faculty at three universities, has presented at numerous conferences and lobbied in Washington D.C. through the AOTA. Richard has published extensively on legal matters concerning healthcare law, legal issues impacting the rehabilitation industry and healthcare public policy.
Presentation Overview
Overview

- **HIPAA** - Health Insurance Portability and Accountability Act of 1996

- **HITECH Act** – Health Information Technology for Economic and Clinical Health Act

- **Texas House Bill 300** (Texas Health & Safety Code Chapter 181)
Why You Should Care

- Healthcare professionals are exposed to protected health information ("PHI").
- **Individual** civil and criminal liabilities.
- **Employer** civil and criminal liabilities.
- Business owners have **obligation**.
- **Vendors** and **subcontractors**.
- **Ethical** considerations.
- Patients have **rights**.
Acronyms You May Hear

- PHI
- HHS
- HIPAA
- OCR
- HITECH
- HB 300
Million & Over in Penalties By Year

- 2017 – avg. $3.16mm
- 2016 – avg. $2.96mm
- 2015/2014 – avg. $2.5mm
- Pre-2014 – avg. $1.55mm
Enforcement Actions

• State attorney generals can enforce; can be awarded attorneys' fees for a successful action.

• **University of Mississippi Medical Center (UMMC)** – protected health information of 10,000 patients affected, $2.75 MM fine; network easily accessed with a “generic” username and password due to stolen laptops.

• **Oregon Health & Science University (OHSU)** – $2.7 MM and 3 year corrective action plan after four breaches compromised the data of more than 3,000 individuals; failed to implement a required security agreement with a cloud service provider where PHI was stored; **no risk assessment**.

• **Catholic Health Care Services (CHCS) of the Archdioceses of Philadelphia** – nursing homes reported to OCR that a CHCS-issued unencrypted iPhone, containing the PHI of 412 individuals was stolen. CHCS agreed to pay $650,000 and enter a two-year corrective action plan.

• **Advocate Health Care Network** – 3 separate breaches affected the ePHI of approximately 4 million individuals; $5.5 MM.
Other HIPAA Breaches & Penalties

- **CardioNet, Inc. (2017)** - provider of remote heart monitoring to pay $2.5 million; stolen laptop with e-PHI of 1391 individuals. No risk assessment or risk management processes. No policies for mobile devices and Security Rule policy in draft form.

- **New York and Presbyterian Hospital and Columbia University (2014)** - twin settlements for $4.8mm; physician deactivation of laptop causing firewall to collapse and release e-PHI. **indication of poor training**

- **St. Joseph Health (2016)** – settlement worth $2,140,500 HIPAA violations compromising e-PHI of 31,800 individuals; failure to recognize the risk of a new server and no enterprise risk assessment.
HIPAA

• **Applies to:**
  – health care providers
  – health plans
  – health care clearinghouses
  – all are COVERED ENTITIES ("CEs") which are required to create and implement certain policies and procedures to protect the privacy and to maintain the confidentiality of patients’ medical information.

• **Four separate HIPAA rules:**
  – Privacy Rule
  – Security Rule *(2003)*
  – Enforcement Rule *(2009)*
  – Final Omnibus Rule *(2013)*
HIPAA

• **The Privacy Rule**: assigns rights to individual patients over their own health information and sets standards covered entities are permitted to *access, use* and *disclose* protected health information (PHI); applies to CEs and business associates (BAs).

• **The Security Rule**: governs the protection of “confidentiality, integrity, and availability of electronic PHI.” Focus is on *standards and implementation of physical, technical and administrative safeguards*.

• **The Enforcement Rule**: provided procedural mechanisms for enforcement of the Rule.
  - Individual notice required within 60 days of when breach if known.
  - Breaches involving 500 or more individuals – notice to DHHS and media.
Implementation Standards for Safeguards

• Three Types of Safeguards:
  – Physical
  – Administrative
  – Technical

• Implementation Standards are either required or addressable
  – Required: speaks for itself
  – Addressable: CE must assess reasonable and appropriate for its environment. Document if not implemented.

• Required – risk analysis, workstation policies, emergency access.

• Addressable – authorization & supervision, access control & validation, encryption.
Understanding HIPAA: What is Protected Health Information (PHI)?

- **Health Data**: information (oral or recorded) in any form or medium created or received by CE, employer, school or public health authority relating to a physical or mental condition of an individual, along with the provision of care and payment.

- **Personal Identifiable Information (PII)**: information identifying an individual, such as name, SS #, DOB, biometric data and account #.

- Combination of health data and PII is considered PHI
  - Applies to both CEs or its BAs.

- **RULE OF THUMB**: Any type of health data (including payment information) that identifies the individual, or there is a reasonable basis to believe it can be used to identify the individual, is PHI.
What Exactly Can Constitute PHI?

- Names, social security numbers, drivers license numbers, address, phone number - if tied to individual health data.
- Photographs, videos, sketches (face, neck, body, scars, tattoos) if can identify and contains health data.
- Audio if can identify and contains health data.
- Details of treatment (health data) if can identify.
- How much detail is enough to turn into PHI is a GRAY AREA.
Complaint Process

• **Complaint → OCR Audit/Intake Review = Resolution, if:**
  – violation did not occur after April 14, 2003
  – entity not covered by the Privacy Rule
  – complaint not filed within 180 days and an extension was not granted
  – incident described does not violate the Privacy Rule

• **If no resolution then: Possible Violation → Investigation → Resolution**

• **Resolution – could mean:**
  – No violation
  – OCR obtains voluntary compliance, corrective action or other agreement.
  – Formal findings of violation = Civil Monetary Penalties (CMPs)

• **Criminal Route: OCR Audit/Intake Review → DOJ → Accepted by DOJ.**
Investigation of Covered Entities

• Cooperate

• Understand your rights and exceptions to the rules – contact a HIPAA compliance expert.

• Allow access to facilities.

• Understand the investigation and subpoena process.
Notice of Privacy Practices

- A health care provider must furnish to each of its patients a notice which explains:
  - (1) how the provider may use the patient’s medical information and how the patient can access his own information – communications, appointment reminders;
  - (2) that federal regulations require the provider to protect the patient’s medical information; and
  - (3) how the patient can report a violation of the patients' rights under the regulations or the providers privacy practices.
Patient Rights

**Theme:**
- Right to access and obtain a copy of their PHI.
- Right to amend their PHI (verify error before change).
- Right to obtain an accounting or listing of disclosures of their PHI.
- Right to receive a Notice of Privacy Practices.
- Right to have communications about their PHI conducted in a confidential manner.
- Right to restrict disclosure on certain uses.
- Right to file a complaint to CE and OCR Office.

**There are EXCEPTIONS to these rules.**
HIPAA: Minimum Necessary Rule

- Identify the **amount of PHI that can be used or disclosed** in a particular circumstance.
- CEs must only share the **minimal amount** of PHI necessary to accomplish the intended purpose.
- Anytime CEs use or disclose PHI, an **evaluation** of minimum necessary is needed.
- **When not to apply**: authorization, treatment, to patient, to Secretary of DHHS, as required by law (subpoena), other standards that comply with HIPAA.
- Vary based on situation; look at **policies & procedures** to define minimum necessary.
Verification

• Create and implement reasonable methods to verify the requesting party is an authorized party.

• Ask questions.

• Establish protocol and point person.

• No single magic formula, but most important is have a process that is reasonable
HIPAA: Use of PHI for Other Purposes

- **Marketing**: a healthcare provider is required to first obtain the patient’s authorization, which must contain a description of the information to be used or disclosed and the name of the person or class of persons who is authorized to use or disclose the information.

- **Business Associates**: a person or entity who performs services on behalf of a covered entity that involves the use or disclosure of protected health information.

- **Business Associate Agreements**: the business associate must agree to protect patient’s medical information in accordance with the provider’s privacy practices and the privacy regulations, as well as provide patients access to their own medical information.
HITECH Act
The Health Information Technology for Economic and Clinical Health (HITECH) Act

- Enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009.
- Contains several changes to HIPAA.
- Intended to promote widespread use and adoption of health information technology which monetary incentives are in place.
- Significantly expand the scope of the privacy and security requirements of the HIPAA privacy and security rules.
- Final Omnibus Rule 2013: breach notifications, increase CMPs and strengthen privacy rights.
Changes Due to HITECH Act

- Direct, statutory liability for business associates for violations of HIPAA’s privacy and security requirements;

- New notification obligations for covered entities, business associates and other organizations in case of breach of personal health information (“PHI”) or protected health records (“PHR”) use and disclosure requirements;

- Additional rights for individuals regarding their PHI, particularly PHI contained in electronic health records.
Changes Due to HITECH Act (cont’d.)

- Additional restrictions on *certain disclosures* by covered entities and business associates;
- Increased *civil penalties* and expanded *criminal liability* for violations;
- *Mandatory compliance audits* by the Department of Health and Human Services;
- An *expansion of entities* required to have business associate agreements; and
- Additional restrictions on *marketing communications*. 
Final Omnibus Rule 2013

• Published January 17, 2013 by DHHS.
• Strengthen HIPAA’s privacy protections and enforcement provisions as required by HITECH.
• Combines four final rules:
  – Modification of the HIPAA Privacy, Security, and Enforcement Rules, including certain mandates by HITECH;
  – Changes to the HIPAA Enforcement Rule’s penalty structure;
  – Updated breach notification rules under HITECH; and
  – Modifications to the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act.
Breach Notification

• **A breach is defined as:**
  – “the acquisition, access, use or disclosure of protected health information in a way not permitted…which compromises the security or privacy of the protected health information.”

• HITECH created the Final Rule *(FR)* for breach notifications.

• A CE who discovers a **breach of unprotected PHI** must notify the affected individuals and the Secretary of DHHS.

• Business Associates *(BAs)* must notify the covered entity.
Breach Notification Changes Due to Omnibus Rule (OR)

• Breaches of “unsecured” health information must be reported – prior to the OR, no such language.

• HITECH require notice to the affected patient and DHHS, if a breach involving patient data carried a significant risk of financial or reputational harm to a patient or patients – uses a “harm” standard.

• **Result under New OR:** the burden of proof is on the covered entity to show that there is a “low probability” that any protected information was compromised.

• Stricter standard assumes a breach from the outset, shifts the burden to the covered entity to show it was not a breach, and removes the discretion of a covered entity to not report based on harm or lack thereof.
Enforcement & Compliance

- **Office of Civil Rights (“OCR”)** is charged with overseeing HIPAA compliance.
- **Pre-HITECH:** Secretary of the DHHS was authorized to impose civil monetary penalties of $100–$25,000 for certain violations of the HIPAA regulations. The Secretary could only impose penalties for knowing violations.
- **Post HITECH:** civil penalties for violations have drastically increased with maximum penalties during any one year of $1.5 million for all violations of a certain type; penalties for violations which were unknown or with reasonable diligence would not have been unknown to the offender.
- State Attorney General’s Office may intervene.
Texas Medical Records Privacy Act (TMRPA)
Who Is a Covered Entity Under Texas Law?

- **TMRPA** drastically changes definition.
- **Any individual, business, or organization** that:
  - Engages in the practice of *assembling, collecting, analyzing, using, evaluating, storing* or *transmitting* PHI;
  - Comes into *possession* of PHI;
  - *Obtains* or *stores* PHI;
  - Is an employee, agent or contractor of a person or entity described above if they *create, receive, obtain, maintain, use* or *transmit* PHI.
TMRPA– Privacy and Security

• TMRPA – aka Texas House Bill 300.

• Health care providers (e.g. SNFs) are considered “covered entities” under TMRPA.

• Employee Training: within 90 days (60 day initial standard-amended in 2013) of anyone getting hired and at least once every two years for ALL employees.
Broad Effects of H.B. 300

- But now also includes less obvious covered entities
  - Law firms and CPA firms that receive PHI;
  - Court reporting firms that receive PHI;
  - Record retrieval that receive PHI;
  - Experts and consultants that receive PHI;
  - Shredding services, storage companies, and other vendors that receive PHI;
- This list goes on…Unless it is a janitorial service having inadvertent contact…then, no worries!
Compliance in Texas: Where to Start?

- HIPAA Risk Assessment – outside vendors can provide;
- HIPAA Compliance (Initial and Ongoing);
- Appoint a HIPAA Compliance Officer;
- Storage/destruction of paper and electronic PHI;
- Data encryption;
- Facility access and security measures;
- Employee training within 90 days of hire and again at least once every two years (employees to sign verification of attendance);
- Mobile device safeguards (passwords, remote wipes, timed lock-outs, Wi-Fi protection);
- And the list goes on…
Who is a Business Associate?

- A person or entity;
- **Not including employees**;
- To whom a covered entity discloses PHI;
- So as to **carry out, assist with, or perform** a function on behalf of covered entity;
- Includes **lawyers, vendors, subcontractors, experts, court reporters, others**…
- Does **not include janitors** with inadvertent contact.
What is a Business Associate Agreement?

• A required contract;

• That provides compliance with HIPAA security rule mandating administrative, physical, and technical safeguards for PHI;

• Must include restrictions on use and disclosure of PHI and set forth mandatory notification to HHS if a PHI security breach occurs.
How is PHI "Secured"?

- PHI can be secured by destroying (renders unusable);
- Or by complying with DHHS encryption guidance standards;
- Proper encryption ultimately avoids the breach notification obligations in event of unauthorized use or disclosure of PHI;
- Secure technical help from vendor specializing in encryption.
What Constitutes "Unsecured" PHI?

- PHI contained in **hard copy** form.
- Electronic storage or transmission of **non-encrypted** PHI.
- Be aware of how you handle this information.
- Hard copies of PHI should **never** be taken to another location (home, office if covered entity is hospital).
- **Faxes** may be problematic.
- **Mobile devices** heighten concern.
What is a PHI "Breach"?

- Any impermissible disclosure of PHI is a breach unless "low probability that PHI was disclosed."
- Examples of possible breaches:
  - Forwarding e-mails outside of hospital/healthcare entities e-mail addresses (to personal accounts), even in peer review context;
  - Stolen or lost mobile devices;
  - Accessing and viewing PHI (electronic trail remains);
  - Disclosing PHI on social media (e.g., possibly sites like Sermo, Medscape, Quantia MD, NY Times Magazine column – depends on how much PHI detail given).
  - Never disclose any PHI to any third party via social media, even with privacy settings.
Where Can PHI Reside?

- Stored/created on a desktop computer;
- Saved to a network server;
- Saved to a USB drive;
- Accessed remotely (by Wi-Fi or otherwise);
- Saved to a cloud shared drive;
- E-mailed to another device;
- Downloaded to a smartphone;
- Printed/stored on a digital copier;
- Printed in hard copy and stored in file drawer.
Policies & Procedures

• Physical office security policies;
• Document retention policies;
• Work station log on and access;
• Network authorization parameters;
• E-mail and calendaring policies;
• Remote access safeguards;
• Protocols for use of mobile devices;
• "Bring Your Own Device" agreements;
• Cloud storage and/or document sharing agreements;
• Portal access agreements;
• Policies for storage, re-use, and disposal of devices.
Don't Do It Because Others Do It

• HIPAA implementation is far from perfect;
• Providers should comply with a higher standard;
• Providers must safeguard PHI of patients;
• Not accessing PHI of patients that are not theirs;
• Even if others do so, this will not provide a defense.

• Example – doctor’s office EHR allowed unauthorized personnel to access other patients; accused of “trolling” and HIPAA violations; EHR showed trail of access.
Disclosing Patient Information Online

• Never disclose:
  – Names, DOBs, contact information,
  – Photographs and x-rays
  – Details of patient care
  – Obtained as a covered entity from a patient

• Patient consent may allow, but **why risk it?**
Audits

- Phase II audits on CEs are complete.
- Phase II audits on Bas are in final stages.
- Phase II did NOT have onsite audits – only desk audits.
- Phase III will be onsite and be broader in scope.

**Prepare:**
- Know regulations
- Have updated policies and guidelines
- Mock audits internally or by third party
- Have access to necessary documentation and know process
Penalties for Violation of HIPAA

- Civil and criminal penalties, but not both for same violation.
- Criminal penalties enforced by the US Department of Justice.
- Civil monetary penalties enforced by the Department of HHS's Office of Civil Rights.
- Criminal penalties only to be imposed when there is proof beyond a reasonable doubt that covered entity and/or business associate knowingly violated HIPAA or any of its regulations.
- Criminal penalties include fines ($100 to $50,000) and/or prison terms (1 year to 10 years).
Penalties for Violation of HIPAA

- Civil complaints will be investigated by the Office of Civil Rights, and can be informally resolved.
- Civil monetary penalties (a hearing may be requested)
  - (1) $100/violation to $50,000 for an unknown violation in spite of due diligence,
  - (2) $1,000/violation to $50,000 for a violation due to "reasonable cause," or
  - (3) $10,000/violation to $50,000 for a corrected violation due to "willful neglect."
  - (4) $50,000/violation for an uncorrected violation due to "willful neglect."
- Court challenge after final HHS Appeals Board decision available.
HIPAA vs. TMRPA

• HIPAA preempts contrary states' laws.
• But HIPAA is a floor.
• States can do more – as shown by HB 300 drastically changing the definition of a “covered entity.”
• HIPAA does not preempt state laws that relate to privacy and security of individually identifiable health information.
• Thus, still need to comply with both the federal laws and any state law that offers more protection for health information.
• Texas offers more privacy protection.
Ancillary Legal Concerns

- Negligence
- Intention Acts
- Employment
- Insurance
- **Litigation Costs**
- Real Property
- Corporate Structure
- Tax
- Corporate Finance
- Intellectual Property
Questions?

Richard Y. Cheng, JD, CHC.
Dykema Cox Smith
214.462.6492
RCheng@dykema.com