SECURETexas
HEALTH INFORMATION PRIVACY & SECURITY CERTIFICATION

Privacy and Security Compliance: Texas & Beyond

HCCA Houston Regional Conference

December 8, 2017

Your Presenters

- **George Gooch**, CEO at Texas Health Services Authority

- **Ed Jones**, COO & CCO at Third Rock, Inc.

- **Sarah Churchill Llamas**, Healthcare IT Attorney & Shareholder at Winstead PC

2

Agenda

1. Welcome
2. THSA Background
3. Texas's Privacy and Security Certification
4. Texas-specific Privacy and Security Regulations
5. Common Mistakes Highlighted in Recent HIPAA Settlements
6. Questions & Answers

Privacy and Security Compliance: Texas & Beyond

Background on the THSA

Texas Health Services Authority
Background

- In 2006, the Texas Health Care System Integrity Partnership, which was convened pursuant to Executive Order RP-61, recommended the creation of the THSA.
- The THSA was created in 2007 by the Texas Legislature through House Bill 1066, now codified in Ch. 182, Health & Safety Code.
- The THSA is a public-private partnership, legally structured as a nonprofit corporation, to promote and coordinate the development of HIE in Texas.
- Governed by a 14-member Board of Directors appointed by the Governor with advice and consent of the Texas Senate.

THSA
TEXAS HEALTH SERVICES AUTHORITY

SECURETexas

5

SECURETexas
HEALTH INFORMATION PRIVACY & SECURITY CERTIFICATION

Privacy and Security Compliance: Texas & Beyond

Texas's Privacy & Security Certification

SECURETexas Certification
Legislative Direction

- Texas HB 300 (82R, 2011) charged the THSA with creating a voluntary certification program.
- Now codified in Section 182.108, Health & Safety Code:
  - Create standards for electronic sharing of PHI;
  - Submit standards to HHSC to be ratified through rule-making process;
  - Establish process by which Texas covered entities may apply for certification of past compliance with standards; and
  - Publish standards on website.

SECURETexas

7

SECURETexas Certification
Standards for Electronic Sharing of PHI

Pursuant to HB 300 (82R, 2011), standards must be designed to:

- Comply with HIPAA and Texas Medical Records Privacy Act;
- Comply with other state and federal law relating to security and confidentiality of information held by a covered entity;
- Ensure secure maintenance/disclosure of personally identifiable health information;
- Include strategies/procedures for disclosing personally identifiable health information; and
- Support level of system interoperability with existing health record databases in Texas.

Those standards are now available at **1 Tex. Admin. Code § 390.2**

SECURETexas

8

SECURETexas Certification
Who is eligible to apply?

- Texas defines "covered entity" much broader than under HIPAA: "Any person who:
  - (A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI. The term includes a **business associate**, health care **payer**, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, **health care provider**, or person who **maintains an internet site**;
  - **(B) comes into possession of PHI;**
  - (C) obtains or stores PHI under this chapter; or
  - (D) is an employee, agent, or contractor of a person described in (A), (B), or (C) insofar as they create, receive, obtain, maintain, use or transmit PHI."

SECURETexas Certification
Preferred Vendor Program

- In an effort to reach all segments of the healthcare sector in Texas, the THSA partners with multiple entities to conduct SECURETexas assessments.
- The THSA began an open enrollment for qualified privacy and security compliance vendors on September 1, 2017, and the period ends December 31, 2017.
- The THSA will conduct this open-enrollment period on at least an annual basis moving forward.

Privacy and Security Compliance: Texas & Beyond

Texas-Specific Standards and Program Details

SECURETexas Certification
Certification Standards

- SECURETexas Certification includes standards for compliance with both **federal** and **state** **privacy and security** standards
  - Thus broader and deeper than a typical HIPAA Security Risk Assessment
- Federal standards include HIPAA, 42 CFR Part 2, and certain other social program requirements (e.g., GINA)
- State standards broken into categories:
  - Requirements for medical records generally (e.g., Texas Medical Records Privacy Act)
  - Requirements specific to data type (e.g., HIV/AIDS, genetic)
  - Requirements specific to providers/facilities/services (e.g., dentists, podiatrists)
  - Requirements specific to certain individuals (e.g., minors)

12

SECURETexas Certification
The Certification Process

- **Review Program Basics.** Visit www.thsa.org/privacy-security-certification. to see if your organization qualifies to apply for certification.
- **Undergo Assessment.** SECURETexas assessments can be conducted through any of the THSA's Preferred Vendors.
- **Remediation.** Correct all high priority and majority of deficiencies identified from the Assessment.
- **Compliance Verification.** Request compliance verification from your Assessor.
- **Obtaining Certification**. Submit all required assessment information to THSA to review for certification. THSA will issue certification letter within 10-15 business days.
- **Renew Certification.** SECURETexas Certification lasts for a period of two years. Entities must report any sentinel events to the THSA as the one-year mark.

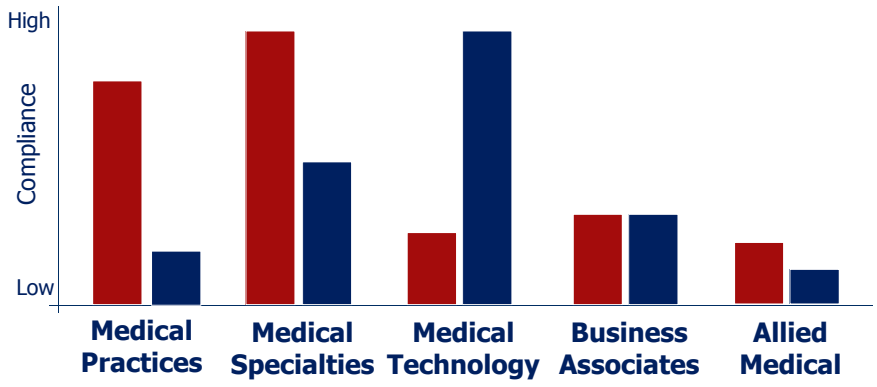
SECURETexas

13

Why is SECURETexas so important?
Healthcare Industry Compliance

- My Observations

Privacy Security



SECURETexas

Industry Trends
Data Security Requirements are Increasing

HIPAA/HITECH
- SP 800-53/66/88….
- Required 1996

Defense Federal Acquisition Regulations
- SP 800-171
- Required 12/31/17

Companies doing business in the European Union
- General Data Protection Regulation (GDPR)
- Required 5/25/18

Financial and Insurance Data Security Law
- Modeled after HIPAA
- Required TBD/2018
- (NY Implemented 2017)

Data security regulations are here to stay!

SECURETexas

SECURETexas Certification
Benefits of Certification

- **Consumer Confidence.** Gives healthcare consumers greater confidence that health information remains protected.
- **Risk Assessment.** Can serve as a security risk assessment, allowing entities to meet HIPAA/HITECH security requirements, MACRA and MIPS.
- **State-Law Mitigation.** Court or state agency shall consider whether the covered entity had SECURETexas certification as a mitigating factor in a proceeding to determine a civil or administrative penalty for a violation of the Texas Medical Records Privacy Act (Chapter 181, Texas Health and Safety Code).
- **HIPAA Mitigation.** Pursuant to 45 CFR 160.408(c), in determining the amount of any civil money penalty, the Secretary will consider . . . "the history of prior compliance with the administrative simplification provisions." The certification report card can provide objective, third-party evidence of this.

SECURETexas

16

Privacy and Security Compliance: Texas & Beyond

Common Mistakes Highlighted in 2017 HIPAA Settlements

Common Mistakes Highlighted in Recent HIPAA Settlements

First HIPAA enforcement action for lack of timely breach notification!

- Entity: **Presence Health Network** - not-for-profit health care system in Illinois consisting of more than 150 locations
- Settlement: **$475,000**
- Facts: Breach: October 2013
  Notification: February 2014 (104 days)
- Bad facts: Investigation of past breaches affecting **under 500** individuals revealed lack of timely breach notification
- "Each day on which Presence Health failed to notify each affected Individual of the breach indicates a separate violation of the Breach Notification Rule."

18

Common Mistakes Highlighted in Recent HIPAA Settlements

Failure to implement safeguards for ePHI

- Entity: **MAPFRE Life Insurance Company** of Puerto Rico
- Settlement: **$2,204,182**
- Facts: USB containing ePHI stolen from IT department affecting **2,209 individuals**.
- Findings:
  - failure to conduct its risk analysis and implement risk management plans,
  - failure to deploy encryption or an equivalent alternative measure on its laptops and removable storage media

"Covered entities must not only make assessments to safeguard ePHI, they must act on those assessments as well" said OCR Director Jocelyn Samuels.

SECURETexas

19

Common Mistakes Highlighted in Recent HIPAA Settlements

Failure to review system activity or implement access controls leads to breach

- Entity: **South Broward Hospital District** d/b/a Memorial Healthcare System, 3rd largest healthcare system in the nation
- Settlement: **$5,500,000**
- Facts: Initial breach report of two employees inappropriately accessing PHI, followed by supplemental report that internal investigation revealed the PHI of **105,646 patients** was accessed.
- Findings: Failure to implement policies to:
  - Regularly review records of information system activity (**audit logs, access reports, and security incident tracking reports**)
  - Establish, document, review and modify user's rights of access

SECURETexas

20

Common Mistakes Highlighted in Recent HIPAA Settlements

Hacker accesses PHI through emails

- Entity: **Metro Community Provider Network**, a nonprofit FQHC with many locations around Denver, CO
- Settlement: **$400,000**
- Facts: Breach reported after hacker accessed employees' email accounts and obtained the PHI of **3,200 patients**.
- Findings:
  - No risk assessment
  - Failure to implement reasonable and appropriate security measures
  - Failure to implement policies and procedures
- Note: Required to conduct risk assessment and develop/implement a risk analysis plan based on the assessment.

21

Common Mistakes Highlighted in Recent HIPAA Settlements

$31,000 for lack of a business associate agreement!

- Entity: **Center for Children's Digestive Health**, a small, for-profit with seven clinics in IL
- Settlement: **$31,000**
- Facts: Failure to have a BAA with a third-party vendor who stored inactive paper medical records. Not having a BAA in place made the disclosure impermissible.
- Lesson: Keep BAAs for at least 6 years beyond the date of when the business associate agreement is terminated.

22

Common Mistakes Highlighted in Recent HIPAA Settlements

Failure to implement access controls

- Entity: **CardioNet, Inc**., provider of ambulatory cardiac monitoring services
- Settlement: **$2.500,000**
- Facts: Notification to OCR of breach of ePHI of **3,500 patients** triggered investigation. Found that they permitted access to PHI on their systems to an unauthorized individual and failed to immediately correct.
- Findings:
  - No risk assessment
  - Failure to establish security management process to prevent, detect, contain and correct security violations
  - Failure to implement policies and procedures governing the receipt and removal of hardware and electronic media that contain PHI in and out of its facilities, the encryption of such media, and the movement of such things.

SECURETexas

23

Common Mistakes Highlighted in Recent HIPAA Settlements

Knowing and intentional failure to safeguard PHI

- Entity: **Memorial Herman Health System**
- Settlement: **$2,400,000**
- Facts: HHS initiated audit after media reports. HHS found MH disclosed **one patient**'s PHI through press releases issues to 15 media outlets and reporters. Further disclosures made to an advocacy group, state representatives, and a state senator. Also disclosed PHI on a statement on its website.
- Findings: Failure to protect PHI, failure to timely document the sanctions imposed against disclosing staff
- Note: Settlement agreement required MH to sanction the involved workforce, including senior level management who failed to comply with privacy and security policies.

SECURETexas

24

Common Mistakes Highlighted in Recent HIPAA Settlements

Careless handling of HIV information jeopardizes patients' privacy

- Entity: **St. Lukes in NYC**, part of Mount Sinai Health System
- Settlement: **$387,200**
- Facts: Investigation after a complaint.
- Findings: St. Lukes improperly disclosed the HIV, AIDS and behavioral health information of **two patients** by faxing their PHI to their employer, and an office at which the patient volunteered, respectively.
- Note: OCR took the type of information disclosed into consideration and stated that the "**impermissible disclosures were egregious**."

SECURETexas

25

QUESTIONS?

- For more information on **THSA**, please visit www.THSA.org
- For more information on **Third Rock**, please visit www.thirdrock.com
- For more information on **Winstead PC**, please visit www.winstead.com

SECURETexas

26