Texas Medical Records Privacy Act (a.k.a. Texas House Bill 300)

Ricky Link, Coalfire

Association of Government Accountants
City Club Bank of America
March 20, 2014

Coalfire®
IT Governance, Risk & Compliance

AGA Dallas Chapter

About Coalfire

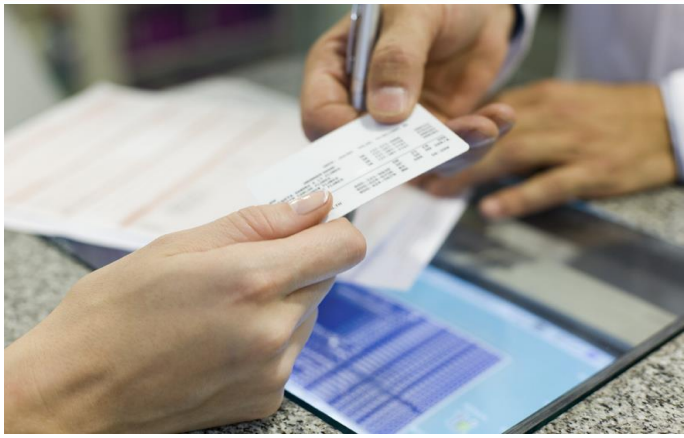
Coalfire offers demonstrated leadership in all key areas in information security, compliance and risk management services for all industries and verticals.

Agenda

- What IS the Texas House Bill 300?
- What are the differences between the Texas Medical Records Privacy Act and HIPAA?
- What are the new compliance requirements?
- What's the current enforcement environment that might affect my organization?
- What are the fines and the penalties for noncompliance?
- How can I defend or avoid a data breach and protect PHI?
- Q&A

Disclaimer – Presentation Not intended To Be An Exhaustive Explanation of HB 300.

Key Learning Objectives

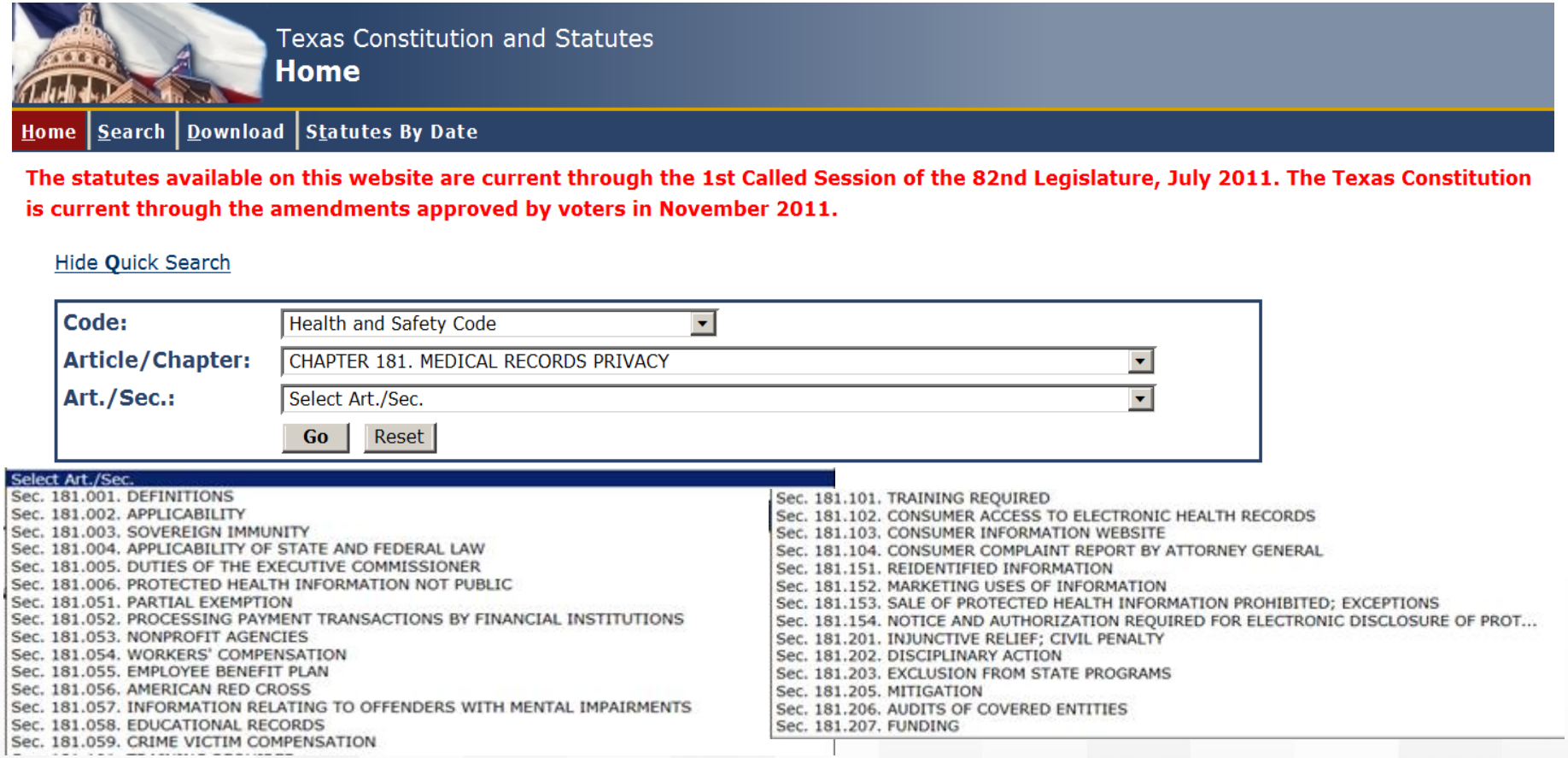


- How to know if their organization is required to comply with the new law?
- What are the requirements for compliance and what do to do in case of a data breach?
- What are the fines and the penalties for noncompliance?
- What's the current enforcement environment that might affect their organization?
- How to defend or avoid a data breach and protect PHI?

Background of
Texas Medical Records Privacy Act
House Bill 300

HB 300 – Where to Find the Texas Statute

www.statutes.legis.state.tx.us



Healthcare Regulation Evolution

HIPAA Act – 1996

- ✓ Signed by Bill Clinton; i.e., Kennedy-Kassbaum Act

HIPAA Privacy Rule – 2003

- ✓ Privacy protections for health information

HIPAA Security Rule – 2005

- ✓ Safeguards for electronic health information

HITECH Act – 2010

- ✓ Security breach notification
- ✓ Enhanced enforcement
- ✓ New requirements for business associates

Texas House Bill 300 – 2012

- ✓ New and additional mandates
- ✓ New fines and penalties

HIPAA Omnibus Rule Released – Jan 2013 (Effective Sept 23…)

- ✓ HIPAA Privacy, Security & Enforcement rules

What IS Texas House Bill 300?

- ***Objective:*** Enhance protections for protected health information (PHI)
- Expands training requirements
- Imposes new restrictions on electronic disclosures of PHI
- Enhances access rights
- Expands security breach notification requirements
- Increases penalties and enforcement

HB 300 – Additional Changes

- The Act broadens the scope of Covered Entities (i.e., called Texas CEs) (Section 181.001(2)):

  - ✓ It applies not only to health care providers, health plans and other entities that process health insurance claims.
  - ✓ Also applies to any individual, business, or organization that obtains, assembles, collects, analyzes, evaluates, stores, or transmits PHI as well as their agents, employees and contractors.

HB 300 – Additional Changes

- Grants enforcement authority to relevant state agencies
  - ✓ Texas Attorney General Office
  - ✓ Texas Health and Human Services Commission
- Creates a consumer website to communicate patient's privacy rights regarding PHI under federal and state (Section 181.103)

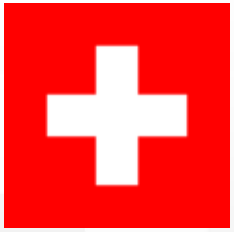
- A list of state agencies that regulate covered entities and the agency's complaint enforcement process (Section 181.104)
- Patient requests for Electronic Health Records must fulfill in 15 days (Section 181.102)

HB 300 – Compliance Challenges

- Poorly drafted
- Substantial ambiguity surrounding scope of coverage
- Substantial ambiguity surrounding certain requirements
- Texas' Office of Attorney General has been inundated with calls
- Informal guidance or regulations might provide additional clarity; however, none provided to date

Discussion Points

What emphasis or differences between HB 300 compared to HIPAA?



HIPAA – Which Providers Are Covered?

Healthcare providers that:

- ✓ Provide care for an individual in the normal course of business; and
- ✓ Engage in standard electronic transactions

Excludes:

- ✓ Providers who do not bill electronically using HIPAA transaction codes
- ✓ "In-house" providers i.e., medical professional on-site

HIPAA – What Health Plans Are Covered?

- Health Insurers and Health Maintenance Organizations (HMOs)
- Employer-sponsored health plans
  - ✓ Group health, vision and dental plans
  - ✓ Pharmacy benefit plans
  - ✓ Healthcare reimbursement flexible spending accounts
  - ✓ Employee assistance programs
  - ✓ Long-term care plans

HIPAA – Who is a Business Associate?

- Business Associates – Those who use PHI to perform, or assist in performing, covered functions for a covered entity. Or who are engaged with processing, storing, or transmission of ePHI…

- The HITECH Act 2010 extended to business associates HIPAA Security Rule requirements and many HIPAA Privacy Rule requirements.

HB 300 – Who is Covered? Definition #1

Any for-profit or non-profit entity that collects, uses, stores, or transmits protected health information, including:

1. "Healthcare facility, clinic, healthcare provider"
   - ✓ HIPAA-covered and non-covered providers
2. "Healthcare Payer"
   - ✓ But only some HIPAA-covered health plans
3. "Business Associates"
4. "Information or computer management entity"
5. "Person who maintains an Internet site"
6. "Schools"

HB 300 – Who is Covered? Definition #2

"Any person who comes into possession of PHI"

1. Sub-contractors to Business Associates
2. Lawyers not acting as business associates
3. Employers – as they may come into possession of PHI (?)
4. Conduits of PHI – ISPs and other telecom providers (?)
5. Someone who finds a CD with PHI on the street (?)
   - ✓ Texas OAG has informally stated that the Texas House Bill 300 does not apply to individuals

HB 300 – Entities Excluded?

Partial Exemption

NOTE: Not exempted from electronic disclosure, marketing, or sale of PHI rules (Section 181.001(4))…

- Employers
- Insurance companies, insurance agents and HMOs

HB 300 – Entities Excluded?

- Employee benefit plans and "any person . . . acting in connection with an employee benefit plan," i.e., business associates to a plan
- Workers' compensation
- Educational records covered by FERPA
- **The American Red Cross**
- Non-profits that pay for healthcare for the indigent and are exempted by regulation by the AG

HB 300 – Summary: Who Is Covered?

Fully Covered

1. All health care providers
2. Business associates to providers and their subcontractors
3. Lawyers and other service providers who are not business associates but do come into possession of PHI
4. Schools with respect to "treatment records"

Partially Covered

1. Employers
2. Insurance companies, insurance agents and HMOs

Interplay of Texas HB 300 and HIPAA

- HIPAA-covered entities must comply with both HIPAA and Texas House Bill 300.

- If there is a conflict between HIPAA and Texas House Bill 300, a HIPAA-covered entity must comply with the “more stringent” standard.

Texas House Bill 300 likely will be more stringent than HIPAA

Texas House Bill 300's New Compliance Requirements

New Training Requirements

1. Section 181.101 – Training must be tail covered entity's particular business, and (b) "each" employee's business activities
2. Training must be completed within ~~60~~ 90 days of hire date (Changed on 6/14/13)
3. Training must be repeated at least bi-annually
4. Employer must obtain and retain a signed statement by each employee verifying attendance
   - ✓ No retention period established in Texas House Bill 300

New Training Requirements

Comparison to HIPAA:

HIPAA (a) does not mandate tailored training, (b) requires training only within a reasonable time, (c) does not require retraining unless there is material change, and (d) does not require a signed verification

Implications:

1. **Existing training policies must be updated**
2. **Existing training materials must be updated**

Electronic Disclosures of PHI – 2 New Requirements

1. **If a covered entity engages in "electronic disclosures" of PHI for any reason, it must post a written notice at its place of business or on its website (Section 181.154).**

- However, there are challenges with these new requirements…

Electronic Disclosures of PHI – 2 New Requirements

2. **Before each individual electronic disclosure, covered entities must obtain the individual's authorization on a form created by the Texas AG (Section 181.154)**
   - Authorization is not required for disclosures (i) to another covered entity for treatment, (ii) for payment or health care operations, or (ii) when required by law

- However, there are challenges with these new requirements…

Electronic Disclosures of PHI – Implications (Section 182.108)

1. Review your organization's disclosures of PHI by electronic means, *e.g.*, email, using a CD or flash drive, through a portal
2. Determine which disclosures are not for Treatment, Payment and Healthcare Operations (TPO) or required by law
3. Identify one or more point persons to control the flow of non-exempt electronic disclosures
4. Train designated point persons on Texas House Bill 300's electronic disclosure requirements

Expanded Access Rights

Healthcare providers that maintain electronic health records must respond to a request for access within 15 business days of receipt of a written request unless HIPAA does not require access

- HIPAA standard is 30 calendar days
- HIPAA permits extensions, but no extensions under Texas H.B. 300

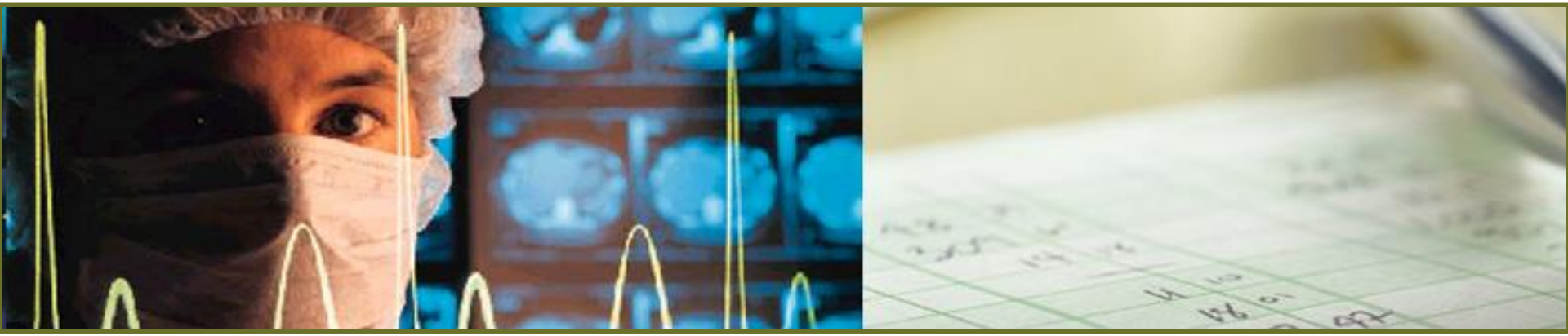
Implications:

Ensure that employees and business associates are aware of the shorter response period

Sales And Marketing Rules (Section 181.153)

1. Sales: No disclosures of PHI for direct or indirect remuneration except as necessary for treatment, payment or healthcare operations
2. Marketing: Covered entity can use PHI for marketing only with individual's prior written authorization
3. Marketing Mailings: If PHI is contained in a marketing mailing, the envelope must show only the individual's contact information, and the mailing must (a) state the name and toll-free number of the entity sending the marketing communication; and (b) explain the recipient's right to have the recipient's name removed from the sender's mailing list.
   - Recipient must be removed from mailing list within 45 days of a request

Enhanced Enforcement



HB 300 – Increased Civil Penalties

Potential maximum civil penalties for breach > 500 patients (Section 181.210):

- **Negligent violations:** $5K/violation/calendar year
- **Intentional violations:** $25K/violation/calendar year
- **Intentional for financial gain:** $250K/violation
- **Pattern or practice:** (a) capped at $1.5M (previously was $250K), (b) revocation of license, and (c) compliance audit
- **Electronic disclosure violations**: Capped at $250K in limited circumstances
- **Texas AG may keep a reasonable portion of the penalty**

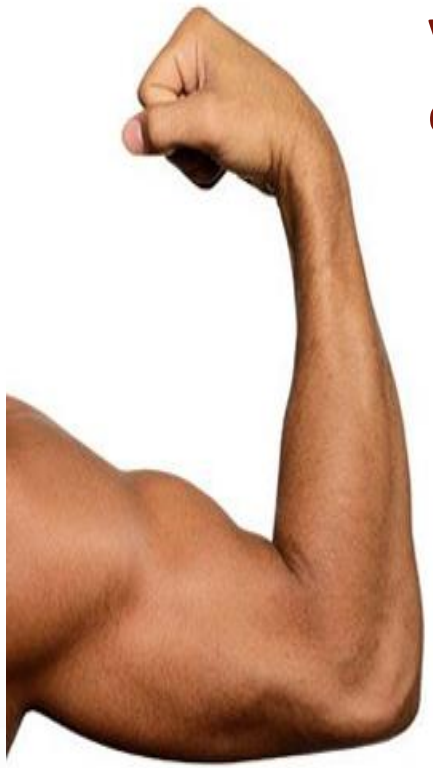
HB 300 – Enhanced Enforcement Mechanisms

- Texas Attorney General must maintain a website which, among other things, contains contact information for each government agency that regulates covered entities and a description of the agency's complaint enforcement process

- https://www.oag.state.tx.us/consumer/hipaa.shtml

- Texas agencies can ask HHS to audit a covered entity's compliance (Section 181.206)

HIPAA – HHS Enforcement



HHS has moved from a philosophy that emphasized voluntary compliance to audits and muscular enforcement

- OCR Pilot audits of 150 covered entities in 2012 (KPMG)
- Audit program becomes permanent in 2013
- $1.5M settlement with Mass Eye & Ear after theft of laptop containing unencrypted PHI of 3,621 patients
- $1.5M settlement with BCBS of TN over the loss of 57 hard drives containing 1M patient records
- $1M settlement with Mass General after employee left 192 patients records on subway

HIPAA – Civil Penalty Enhancement

- **Minimum penalties if violation is not corrected within 30 days of notice of the violation**
  - ✓ Unknowing Violations: $100 per violation and $25,000 annually
  - ✓ Negligent Violations: $1,000 per violation and $100,000 annually
- **Willful Neglect: "Conscious intentional failure or reckless indifference to the obligation to comply"**
  - ✓ $10,000 per violation and $250,000 annually (if corrected within 30 days)
  - ✓ $50,000 per violation and $1.5M (if not corrected)

Expect More Civil Enforcement

State attorneys general can sue in federal district court to recover damages to state residents caused by a HIPAA violation

- ✓ TX AG has obtained settlements from numerous entities for alleged improper destruction of PHI and other sensitive personal information.
- ✓ 07/11/12: Indiana AG announces that WellPoint agreed to pay $100k to settle charges that the company had unreasonably delayed security breach notification.
- ✓ 07/10/12: CT AG announces settlement with HealthNet over its loss of a computer disk drive containing the PHI of 1.5M individuals nationwide. HealthNet to (a) implement Corrective Action Plan, (b) pay $250K fine, and (c) make additional $500K payment if it is determined that PHI on lost disk was misused.

How can I defend or avoid a data breach and protect PHI?

Audits and Risk Assessments

- The state will direct federal audits to be conducted by the Department of Health and Human Services.

  If the state identifies evidence of violation, the covered entity may be required to submit a written risk analysis to determine if the violation qualifies for enforcement action.

- As with any compliance requirement, covered entities should maintain a current risk assessment that demonstrates the level of protection provided to patient data.

  This may prove that any failure to protect patient data would have been an exception to policy and not a pattern of neglect.

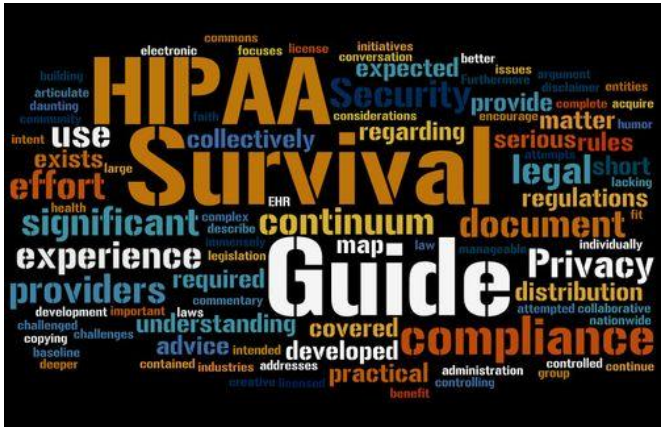
- Evidence of Good Faith efforts to comply with HB 300 is recommended

Data Breach Notification

- Data breach notification is already a part of Texas code.
- Texas House Bill 300 specifically requires covered entities to provide notice of breach that meets specific unauthorized disclosure thresholds.

- An entity must disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized individual.
- The disclosure must be made as quickly as possible or as necessary to determine the scope of the breach and restore the reasonable integrity of the system.
- Penalty: $100/individual/day that notice is not sent, capped at $250K

Five Simple Steps to Compliance



1. Establish a risk management program to support
   protection of sensitive patient data.

2. Document policies and controls regarding patient access to their EHRs to mitigate risks.

3. Train users to implement the controls and privacy program.

4. Deploy a breach notification and incident response plan.

5. Conduct a periodic assessment of the controls and risk management program to demonstrate effective oversight (i.e. avoid claims of a pattern of neglect).

Tools and Resources

1. Health IT Resources – Consolidated from Best Practices; downloadable tools:
   - www.healthit.gov/providers-professionals/ehr-privacy-security

2. Regional Extension Centers:
   - www.TXrecs.org

3. Texas HIT Connection:
   - http://texasqio.tmf.org

Questions

Ricky Link, Coalfire Systems
Managing Director, Southwest Region
Ricky.Link@coalfire.com
972.763.8011

Visit the Coalfire blog:
www.coalfire.com/The-Coalfire-Blog