



HIPAA or HIPPA???

Which one??



HIPAA!!!!

HIPAA stands for the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct and is a U.S. federal law enacted in 1996 as an attempt at incremental healthcare reform. It was subsequently revised in 2009 with the ARRA/HITECH Act and again in 2013 with the Omnibus Rule.

Who Needs to Comply with HIPAA???

Any organization or person who works in or with the healthcare industry or who has access to protected health information.

Texas H.B. 300

- In June of 2011, Texas H.B. 300 was passed in Texas and went into effect September 2012.
- This bill goes above and beyond the federal HIPAA Privacy and Security Rules.

Why do Texans need to know about
this?

BECAUSE THE ATTORNEY GENERAL ENFORCES TEXAS HOUSE BILL 300!!!!

Who is Required to Comply with Texas HB 300?

- Compliance with Texas HB 300 is mandatory for all covered entities that are based in Texas or do business with Texas residents. Covered entities under Texas HB 300 differ from covered entities as defined in HIPAA.

Who is Required to Comply with Texas HB 300?

- Texas HB 300 expanded the HIPAA definition of covered entity (healthcare providers, health plans, and healthcare clearing houses) to include any entity or individual that possesses, obtains, assembles, collects, analyzes, evaluates, stores, or transmits protected health information in any form.
- Texas HB 300 therefore applies to all healthcare organizations, including those that are not covered by HIPAA, and also lawyers, schools, universities, researchers, accountants, Internet service providers, IT service providers, government agencies, and individuals who maintain a website that collects, stores, or interacts with PHI.

Texas HB 300 Exemptions??

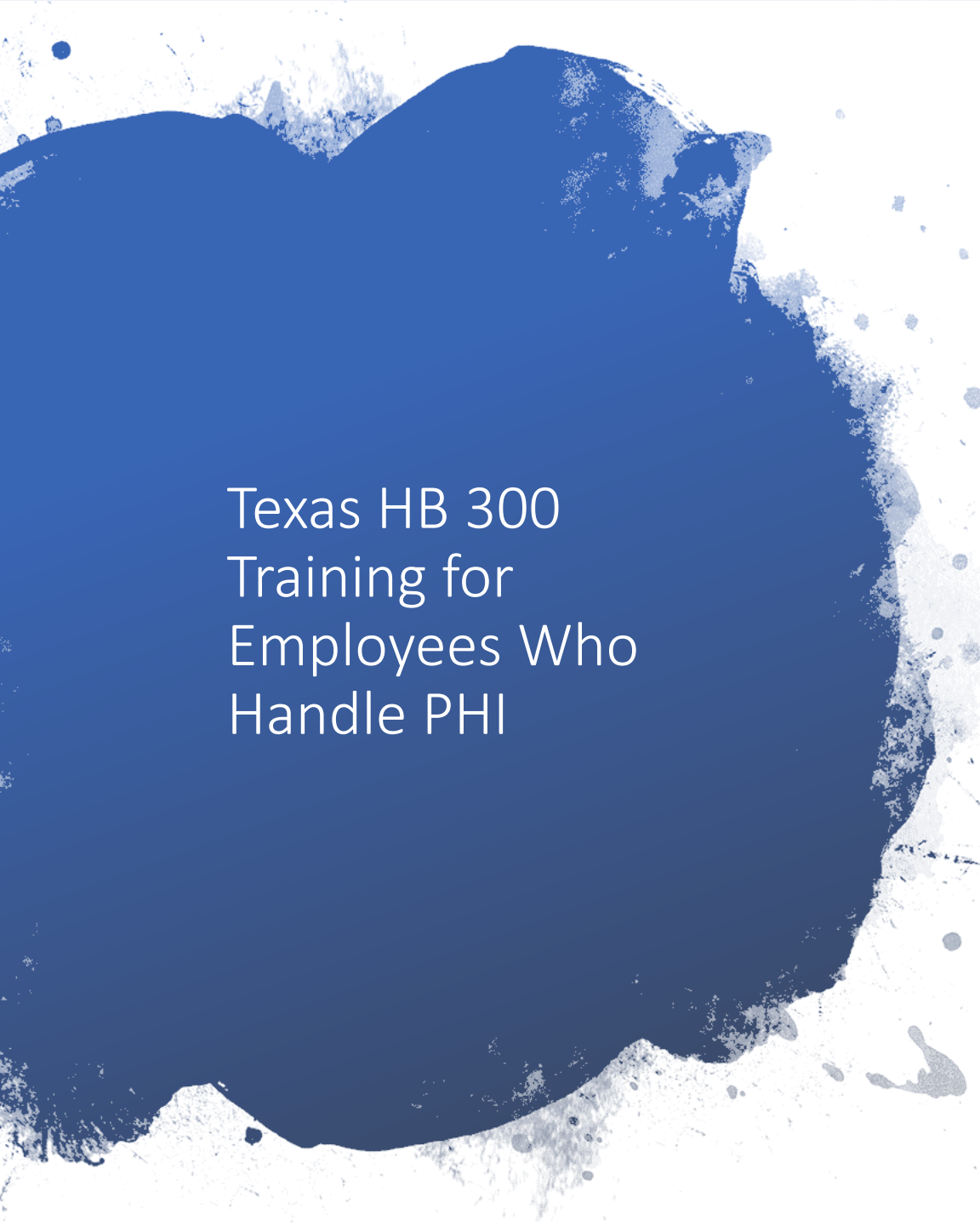
- Not-for-profit agencies that pay for healthcare services or prescription drugs for indigent persons if the primary business of the agency is not the provision of healthcare services or reimbursement for healthcare services.
- Workers' compensation insurance and any entity or individual who acts in connection with the provision, support, administration, or coordination of benefits under a self-insured workers' compensation program.

Texas HB 300 Exemptions??

- Employee benefit plans and entities or individuals that act in connection with those plans
- Entities or individuals that provide, administer, support, or coordinate benefits associated with compensation for victims of crime.
- Processing of certain payment transactions by financial institutions and education records covered by the Family Educational Rights and Privacy Act of 1974.

Texas HB 300 and Electronic Health Records

- Texas HB 300 introduced new standards for handling electronic health records. A covered entity is prohibited from using PHI for any reason other than the provision of treatment, payment for healthcare, or insurance purposes unless, prior to the disclosure of PHI, the covered entity has obtained written authorization from an individual to disclose their PHI.
- HIPAA requires covered entities to provide patients and plan members with copies of their PHI on request and those requests must be honored within 30 days of the request being submitted. Texas HB 300 requires covered entities to provide copies of PHI much more rapidly – Within 15 days of a written request being received.



Texas HB 300 Training for Employees Who Handle PHI

All employees who are required to handle PHI or Sensitive Personal Information (SPI), or are likely to encounter PHI, are required to undergo formal privacy training within 60 days of commencing employment. In contrast to HIPAA, which does not stipulate how often additional training must be provided, Texas HB 300 requires additional privacy training to be provided at least every two years. Training sessions need to be tailored to the role and responsibilities of the employee. All training must be documented and employees are required to sign to confirm that they have received the training.

Texas HB 300 Penalties for Noncompliance?

- **Tier 1:** Up to \$5,000 per violation, per year, for violations due to negligence
- **Tier 2:** Up to \$25,000 per violation, per year, for a knowing or intentional violation
- **Tier 3:** Up to \$250,000 per violation, per year, for an intentional violation for financial gain
- The maximum financial penalty is \$1.5 million per year in cases where there has been a pattern of noncompliance.

Protected Health Information (PHI)

Can PHI be sold???



NO!!!! PHI must never be sold. It is against the law!!!

A covered entity may disclose PHI to another covered entity when:

A patient has authorized it

Performing an Insurance or HMO function

Authorized/required by federal or state law

Covered
Entity?

Engages in assembling, collecting,
analyzing, storing or transmitting PHI

Comes into possession of PHI

Obtains or stores PHI

Or is an employee, agent, contractor of one
described above

Examples

- Medical workers – social, mental health, administrators, etc.
- Medical Records people
- Therapists – marriage or family
- Counselors – substance abuse or chemical dependency
- Embalmer/funeral director

Business Associate?

- An entity or person, other than a staff member of a covered entity, who performs activities, functions, or provides certain services which involve access to PHI or e-PHI from a Covered Entity
- A business partner of a Covered Entity that does things for or in the operating environment of the Covered Entity's Business

Business Associate?

- Any downstream subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate, even if they have an indirect relationship with a covered entity, is included in being required to adhere to HIPAA.

Examples of Business Associate



Answering Services



Attorneys



Billing companies



Collection agencies



Record storage
companies



Shredding
companies



Transcription
services



Court
reporters/court
reporting firms???

Texas HB 300 Training Requirements

- Covered entities must provide their employees with customized federal and state privacy and security law training within 90 of employment
- Privacy and security training must be repeated every 2 years unless there is a material change concerning PHI
- Covered entities must document privacy and security training whether it is electronic or written format for each employee and maintain signed statements of completion

Texas HB 300 Training Requirements

- Covered entities must provide their employees with customized federal and state privacy and security law training within 90 days of employment
- Privacy and security training must be repeated every 2 years unless there is a material change concerning PHI
- Covered entities must document privacy and security training whether it is electronic or written format for each employee and maintain signed statements of completion

In Summary

- According to [HIPAA privacy standards](#), court reporters and court reporting firms are required to keep PHI and PII in each case “protected in a manner that the witness (et al.) is afforded full confidence that their information is secure.” The law deemed court reporters and court reporting firms as “business associates” in the litigation discovery process due to their exposure to and handling of privileged and confidential client information.