Texas Health and Safety Code, Chapter 181
Medical Records Privacy Law, HB 300

Training Module provided as a component of the Stericycle HIPAA Compliance Program
Goals for Training

• Understand how **Texas House Bill 300 (HB300)** significantly expands State’s Patient Privacy Protections and imposes new requirements on Covered Entities (CEs)

• Learn what the new law requires:
  ✓ Mandatory employee training
  ✓ Informing patients about how their electronic Protected Health Information (ePHI) is used and disclosed
  ✓ Providing patients with EHRs within 15 business days after receipt of a written request
  ✓ Prohibition on sale of PHI
  ✓ Texas Attorney General website and annual report to the Texas Legislature on patient complaints over medical privacy
  ✓ Increased enforcement penalties

• Notification Requirements if PHI is wrongfully disclosed

• Best Practices for safeguarding Protected Health Information (PHI)
Why was House Bill (HB) 300 introduced?

• HB 300 was introduced in response to a large data breach that exposed the personal information of 3.5 million Texas residents—the breach was discovered in March 2011.

• Information was discovered on a government server accessible to the public:
  • The breach included:
    ➢ Names
    ➢ Mailing addresses
    ➢ Social security numbers
    ➢ Dates of birth
    ➢ Driver’s license numbers

• In response to the breach, the Texas attorney general’s office and the FBI launched a criminal investigation.
The State of Texas Responded by:

- Immediately securing the information and moving it to a private location
- Contacting all three major credit reporting agencies
- Arranging for one year of credit monitoring at no charge for those whose information was affected
- Notifying media outlets through a press release; and
- Creating a website to provide information to those affected

[www.tx safeguard.com](http://www.tx safeguard.com)
Texas Governor Rick Perry signed **HB 300**, which modified the Medical Records Privacy Law, in June 2011 with an **effective date of September 1, 2012**.
Highlights on the Changes:

- Requirement that **all covered entities**, as defined under Texas state law, comply with HIPAA
- **Mandatory training** for employees regarding protected health information (PHI)
- **Greater patient rights** to electronic medical records
- **Separate authorization** for electronic disclosure of PHI
- **Shorter timeline** to provide patient with electronic copy of EHR
- **Prohibition on sale of PHI**
- **Broader scope** and guidelines for breach notification
- **Stricter penalties, increased fines** for non-compliance
The Administrative Simplification standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is:

- a health care provider that conducts certain transactions in electronic form*
- a health care clearinghouse
- a health plan

*Covered transactions are transactions for which the Secretary has adopted standards; the standards are at 45 C.F.R. Part 162.
Under Texas law, a Covered Entity means any person who:

- For any purpose engages in the practice of assembling, collecting, analyzing, using, evaluating, storing or transmitting of Protected Health Information, (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;
- Comes into possession of PHI
- Obtains or stores PHI
- Is an employee, agent, or contractor of a CE who in their capacity as such receives obtains, maintains, uses or transmits PHI

The definition of a Covered Entity under *Texas Health and Safety Code, Chapter 181, Medical Records Privacy* is broader than federal HIPAA’s definition.
While still considered Covered Entities, the provisions of Chapter 181 of the Texas Health and Safety Code do NOT apply to:

- Worker’s compensation plans and the people who administer self-insured worker’s compensation plans
- Employee benefit plans and the people who administer them
- The American Red Cross from accessing any information necessary to perform their duties
- Educational records covered by the Family Educational Rights and Privacy Act
- Non-profit agencies who pay for care of indigent people but whose primary business is not the provision of health care or reimbursement for health care
- Processing of certain payment transactions by financial institutions
- Certain information relating to offenders with mental impairments
Implications of Texas’ Expanded Definition of a Covered Entity

- **Additional requirements** for CEs:
  - Mandatory Compliance Training
  - Electronic Disclosure Notice
  - Authorization for Electronic Disclosure of PHI
  - Provision to provide EHR within 15 business days
  - Enhanced penalties for breaches

- Chapter 181 of this law has specific **restrictions** on the use of PHI for Marketing purposes

- **Audits** of CEs

- **Broader scope** for breach notification

**Effective Date** – September 1, 2012
Mandatory Training Requirements

• HB 300 requires CEs to train employees on their obligations under federal HIPAA and state of Texas privacy and security law—Within 60 days of employment

• Training is required to be repeated every two years

• Training sessions require a sign in sheet verifying attendance
HB 300 provides a requirement that CEs who create or receive PHI regarding individuals must provide notice to individuals if their PHI is subject to electronic disclosure.

General notice may be provided by:

- Posting a written notice in the CE’s place of business
- Posting a notice on the CE’s Internet website; or
- Posting a notice in any other place where individuals whose PHI is subject to electronic notice are likely to see the notice
HB 300 provides that a CE cannot electronically disclose an individual’s PHI to any person without **a separate authorization** from the individual or their legal authorized representative **for each disclosure**, unless the disclosure is to another CE, for one of the following purposes:

- Treatment
- Payment
- Health care operations
- Performing certain insurance or HMO functions; or
- As otherwise authorized or required by state or federal law
Texas law requires CEs to provide patients with electronic copies of their EHR within 15 BUSINESS DAYS of the patient’s written request for the records.

- A health care provider using an electronic records system “capable of fulfilling the request” must provide a person with an electronic copy (unless the requesting individual accepts an alternative form) of the person’s electronic health care record.

- The Health and Human Services Commissioner, in consultation with the Texas Health Services Authority (THSA), the Texas Medical Board and the Texas Department of Insurance is charged with recommending a standard electronic format for the release of requested health records.
The Sale of PHI is Prohibited

CEs may not disclose PHI to any other person in exchange for “direct or indirect” remuneration or financial gain.

- There is an exception for disclosure from one CE to another, if:
  - For treatment, payment; health care operations, certain insurance and HMO functions, or as otherwise authorized or required by law; and
  - Provided that costs cannot exceed reasonable costs of preparing or transmitting the PHI
Breach Notification Requirements

Under HB 300, any business (not just a Covered Entity) that conducts business in Texas and handles PHI must provide notification to Texas residents if their PHI is wrongfully disclosed.

- HB300 extends breach notification to any impacted individual, whether in Texas or elsewhere.
- Applies to recipients in Texas or in states that do not have breach notification requirements.
- Any business that fails to make the required notification is subject to state penalties not exceeding $250,000 for a single breach.
- HB 300 makes it a state jail felony for individuals who use a scanning device or other re-encoder to access, read, scans, store or transfer PHI without authorization.
Penalties for Breaches by a Covered Entity

• The Texas State Attorney General’s office may institute an action for civil monetary penalties not to exceed:
  - $5,000 per violation per year if negligent
  - $25,000 per violation per year if done knowingly or intentionally
  - $250,000 for each violation if knowingly or intentionally used PHI for financial gain
  - A pattern or practice of abuse can result in penalties up to $1.5 annually

Similar penalties can be assessed by Health and Human Services under HITECH and the HIPAA Omnibus Final Rule.

• When determining a penalty, the Texas State Attorney General will take into account:
  - the seriousness of the violation
  - the CE’s compliance history
  - the risk of financial, reputational or other harm to the affected patients
  - the amount necessary to deter future violations
  - any efforts taken by the covered entity to correct the violation
Audits of Covered Entities

• The state of Texas through The Texas Health and Human Services Commission (HHSC) can:
  – Request federal authorities to audit HIPAA covered entities to determine compliance under HIPAA
  – Periodically monitor the results of audits of Covered Entities

• If the HHSC has evidence that the CE has engaged in violations that are egregious and constitute a pattern or practice, the HHSC may:
  – Require the CE to submit results of a risk analysis to the HHSC; or
  – If the CE is licensed by a state agency, request the licensing agency to perform an audit of the CE
• The Texas Attorney General must maintain a website describing patient privacy rights under state and federal law and publish an annual report detailing privacy complaints filed with state agencies during the previous year.
Key Takeaway

- Texas is serious about protection of personal privacy
- Entities need to encourage a culture of compliance that values and promotes the protection of private information

The cost of a breach can be staggering.

Failing to comply with HIPAA, the HITECH Act and HB 300 can lead to potentially significant financial penalties and these costly repercussions:

- Reputational
- Financial
- Legal, Regulatory
- Operational
- Clinical
Caution must be taken to secure patient information and dispose of PHI no longer needed:

• **When you step away from your desk or workstation:**
  – ensure that you secure your mobile device, lock your workstation
  – close files, turn over or secure any paperwork that may contain PHI

• **When you leave for the day:**
  – ensure that you lock any PHI in the appropriate file cabinets and/or desk drawers of your work area

• **When you need to dispose of PHI no longer needed:**
  – Place PHI in a secure bin for shredding or shred documents with PHI immediately when no longer needed
  – PHI should never be placed in the regular trash
1. Do not share passwords
2. Use strong passwords
3. Do not write down passwords by unsecured means
4. Never use another person’s login credentials
5. Never take pictures of patient information with your cell phone or tablet camera
6. Never allow patients to use or gain access to Organization computers or devices
7. Be aware of threats to your computing environment (malicious software, viruses, etc.)
8. Follow your Organization’s data security policies for:
   • Accessing data
   • Storing data
   • Transmitting data
   • Destroying data
   • Use of external media
The confidentiality and security of a patients’ PHI is your responsibility—please protect it wisely!