HB 300

Texas Medical Records Privacy Law
Overview

• Effective September 1, 2012
• Texas Health and Safety Code: Chapter 181
  (Medical Records Privacy)

1. **Greater enforcement and increased penalties**: broader definition of covered entity;$5,000 per violation to $1.5 million per year

2. **New operational requirements**: training, notice, disclosure, authorization, breach notification
Acronyms

- CE = covered entity
- PHI = protected health information
- EHR = electronic health record
- TPO = treatment, payment, and health care operations
- HHSC = Health and Human Services Commission
- THSA = Texas Health Services Authority
- AG = Texas Attorney General
181.001: Covered Entity

- CE under HIPAA, you must comply.
- CE under Texas law, you must comply.

181.001(b)(2) "Covered entity" means 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 protected health information. 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 protected health information;
  — (C) obtains or stores protected health information under this chapter; or
  — (D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information."
Enforcement and Penalties
# 181.201 Civil Penalties

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>HB 300</th>
</tr>
</thead>
<tbody>
<tr>
<td>$100 per unknowing violation, up to $50,000</td>
<td>$5,000 per negligent violation</td>
</tr>
<tr>
<td>$1,000 per violation without willful neglect, up to $50,000</td>
<td>$25,000 per knowing violation</td>
</tr>
<tr>
<td>$10,000 per violation due to willful neglect, up to $50,000</td>
<td>$250,000 per violation made for financial gain</td>
</tr>
<tr>
<td>Penalty capped at $1.5 million annually</td>
<td>Penalty capped at $250,000 annually if certain mitigating factors are met or $1.5 million* annually if there is a pattern of violations</td>
</tr>
</tbody>
</table>
181.201 Civil Penalties cont.

• Mitigating factors related to the penalties ranging from $5,000 - $250,000:
  – The seriousness of the violation;
  – The entity’s compliance history;
  – Whether any harm was done to the individual involved in the violation;
  – Whether the covered entity had participated in THSA’s certification process;
  – How much of a fine might be needed to deter future violations; and,
  – The covered entity’s efforts to correct the violation.
181.201 Civil Penalties cont.

Mitigating factors related to the $250,000 annual cap:

- Court must find:
  1. The disclosure was made **only** to another CE **AND** **only** for the following reason(s):
     - TPO or performing an insurance or HMO function; OR
     - As otherwise authorized or required by state or federal law.
  2. The PHI was:
     - Encrypted or transmitted using encrypted technology;
     - The recipient of the PHI did not use or release the PHI; OR
     - At the time of the disclosure the CE had implemented policies on the use of PHI.
181.201-202 Civil Penalties cont.

• State licensing agency can investigate and revoke license if violations are found to be a pattern or practice and egregious.

• NEW: State licensing agency can refer cases to the AG’s office for further action and civil penalties. The AG may retain a portion of the civil penalties recovered.

• A violation by an individual or facility licensed by an agency of the state is subject to disciplinary proceedings, including probation or suspension by the licensing agency. If there is evidence that violations are egregious and constitute a pattern or practice, the agency may:
  – Revoke the CE’s license; OR
  – Refer the case to the AG for civil penalties.
181.205 Mitigating Factors

• In any action or proceeding to impose an administrative penalty or assess a civil penalty for actions related to the disclosure of PHI, a CE may introduce, as mitigating evidence, evidence of the CE’s good faith efforts to comply with:
  – (1) state law related to the privacy of individually identifiable health information; or
  – (2) HIPAA.
New Operational Requirements
181.101 Training

• Requires CEs to provide training *every two years* about state and federal laws on protected health information *related to the line of business and the employee’s scope of employment*. Training must be completed within in 60 days of hiring, and documented.
181.154 Notice

• CEs must provide individuals with general notice that their PHI may be *electronically* disclosed.

• Notice may be posted:
  – In their place of business;
  – On an Internet site; or
  – Any other place an individual may be likely to see it.
181.154 Authorization

• **General Rule:** A CE may not electronically disclose an individual’s PHI to any person without a *separate authorization* from the affected individual or the individuals legally authorized representative for *each* disclosure. Authorization may be in written or electronic form, or orally given (if documented).

• **Exceptions:** Authorization is not required if:
  1. The disclosure is made to another CE for the purposes of TPO or performing an insurance or HMO functions; OR
  2. As otherwise authorized or required by state or federal law.

• Not later than Jan. 1, 2013, the AG shall adopt a standard authorization form which must comply with HIPAA and state law.

NOTE: The notice and authorization requirements do not apply to a CE as defined in Ins. Code § 602.001 if that entity is not a CE under federal law or Tx. Health and Safety Code Chapter 181.
181.153 Disclosure of PHI

• **General Rule:** A CE may not disclose PHI for direct or indirect remuneration.

• **Exceptions:** Disclosure of PHI to another CE for remuneration is allowed for:
  1. TPO;
  2. Performing an insurance or HMO function; or
  3. As otherwise authorized by or required by state or federal law.
     – If a CE received payment for PHI, the amount may not exceed the CE’s reasonable costs of preparing or transmitting the information.
181.102 Request for Patient Record

• **General Rule:** A health care provider using an electronic health records system *capable of providing an electronic record to a consumer* must fulfill a request for an electronic copy of a person’s record in *no more than 15 business days AND in electronic form*, unless the person agrees to accept another form.

• **Exceptions:** Federal exceptions to release of PHI under HIPAA apply.

• Texas HHSC *may* recommend a standard electronic format for the release of EHRs, and it must be consistent with federal law, if feasible.
181.206 Auditing

- Texas HHSC may request that the U.S. Secretary of Health and Human Services perform an audit of a CE in Texas to determine HIPAA compliance. HHSC must monitor results of request.
- *If Texas HHSC has evidence that a CE has committed violations that are egregious and constitute a pattern or practice,* HHSC may require the CE to perform and submit a risk analysis. Texas HHSC may, alternatively, refer a CE to a licensing agency for an audit.
- Texas HHSC must report to the Texas Legislature on the number of federal audits conducted.
Business & Safety Code § 521.053
Breach Notification

• Breach notification is required to Texas residents AND residents of a state that does not have its own breach notification law.

• If the individual impacted is a resident of a state that does have its own related breach notification law, notice under that state’s law satisfies the Texas requirement.

• Penalties for Failure to Comply with Breach Notification:
  – Civil penalty of not more than $100 for each person for each day in which the CE does not take “reasonable action” to notify the individual (cap of $250,000 for all individuals under a single breach).
182.108 and Ins. Code § 602.054
Texas Health Services Authority

• THSA is tasked with:
  – developing privacy and security standards for the electronic sharing of PHI; and,
  – developing a *voluntary* certification process for CEs that want to use the standards.
Additional provisions

• AG must maintain a website with information on consumer privacy rights and other information. Website must be up by May 1, 2012. AG must annually report to the Texas Legislature on all consumer complaints received and their enforcement action taken, if any. Other Texas agencies must report any complaints received to the AG for this report. The first report is due by Dec. 1, 2013

• Texas HHSC shall explore and evaluate new developments in protecting PHI and report by Dec. 1 each year to the legislature.

• Texas HHSC review issues related to the security and accessibility of medical records held by a CE that ceases to operate.

• A task force of 11 members shall be created to develop recommendations for improvement of informed consent protocols, the improvement of patient access to PHI, and any other critical issues related to PHI.

• An identify theft offense that involves stealing PHI is now a state jail felony.
Questions?

References:
To find HB 300 (82): http://www.capitol.state.tx.us/
To find Tx. Health and Safety Code:
 http://www.statutes.legis.state.tx.us/Index.aspx