The differences between HIPAA and HB300 in Texas

In the event of a conflict between HIPAA and state law, whichever is more strict is the one to follow.

HB300 was passed in May of 2011. This law imposes requirements regarding training, electronic health records access, sales of protected health information, notice and authorization for electronic disclosures, enforcement and disciplinary actions and audits. Here is the statute: https://statutes.capitol.texas.gov/?tab=1&code=HS&chapter=HS.181&artSec=

With HIPAA, a covered entity is generally considered a health plan, health care clearinghouse, or health care provider who transmits and health information in electronic form.

A "covered entity" in Texas basically covers everyone who has possession of protected health information. All healthcare facilities are covered by HB300, even if they're not covered by HIPAA. Additionally, it's any person, business or entity who possesses, assembles, collects, analyzes, uses, evaluates, stores or transmits protected health information. This includes business associates, healthcare payers, lawyers, accountants, universities, computer management companies, schools, researchers, healthcare providers and internet site providers, as well as their employees, contractors, or agents. So, some of these folks may not be subject to HIPAA laws and penalties, but they are subject to the Texas law. That being said, please note that a breach could result in both HIPAA and HB300 penalties.

Each covered entity must train its employees on state and federal laws regarding PHI within 90 days after the employee is hired, and must be done every two years, plus any time a change to the law or a change to the office policies and procedures occur. (Although most federal HIPAA experts say it needs to be done every year (along with an annual risk assessment). According to HIPAA, training must be done regularly, which most HIPAA experts recommend on an annual basis. Training sessions need to be tailored to the role and responsibilities of the employee and the interactions they are likely to have with patients PHI. The training should cover the requirements of the legislation, how it increases protections for health information, the types of information covered, how HB 300 relates to medical record access by employees, how healthcare data must be protected, patient authorizations for electronic disclosures of PHI, the reporting of potential violations and the penalties for violations. Training must be documented and the covered entity must maintain these signed statements for six years, even if the employee is no longer a current employee. (HIPAA requires training, but has no specific guidelines about frequency.)

If a patient requests a copy of a record, it must be provided within 15 days (30 for HIPAA, but it will probably also be changed to 15 days). Yes, even if they owe you money. An authorization must be obtained for each disclosure unless it's specifically exempted in section 181.154 https://statutes.capitol.texas.gov/Docs/HS/htm/HS.181.htm (The HIPAA rules allow for some disclosures with patient verbal consent or if the disclosure is considered to be in the best interest of the patient.)

A covered entity generally cannot use information for anything other than treatment, payment healthcare operations, performing an insurance or health maintenance organization function. The information must be provided in the form/format requested by the patient. If the PHI is not available in that format, either a hard copy must be provided, or another format agreed upon by the patient. If the information is to be used for any other purposes, an authorization must be obtained.

Notice and Authorization is required if patients' information may be disclosed. A notice that discusses how patients' information may be disclosed must be posted in the office, on the website, and/or in any other place where individuals, whose PHI is subject to disclosure, will likely see the notice.

A covered entity may not electronically disclose information without patient authorization, unless the disclosure is for treatment, payment, or health care operation purposes. The authorization may be in written, electronic, or oral form; so long as the covered entity documents it in writing. (HIPAA requires that authorizations be in writing and certain elements must be included, so I would always obtain a written authorization that complies with the HIPAA

requirements.) The PHI can be sold without patient authorization when the sale is to another Covered Entity for treatment, payment, health care operations, or insurance/health maintenance operation.

Civil penalties for negligent violations range from $5,000 up to as much as $1.5 million per year when there is a pattern of non-compliance. They now have a tiered penalty structure:

- Tier 1: Up to $5,000 per violation for violations due to negligence
- Tier 2: Up to $25,000 per violation for a knowing or intentional violation
- Tier 3: Up to $250,000 per violation for an intentional violation for financial gain

Penalties are based on the seriousness of the violation, compliance history, the intent of the behavior, whether harm occurred, and whether measures have been taken to correct the problem.

A covered entity may also receive discipline from the Board, including license revocation and exclusion from any state programs.

The law provides that covered entities may be audited by the HIPAA folks, in coordination with the Texas Attorney General, the Texas Health Services Authority, and the Texas Dept. of Insurance. They may require a copy of the entity's risk analysis and may bring in the Board to conduct an audit, as well.

The Bill also increased covered entity's obligation to protect information that could be used for identity theft, including name, date of birth, social security number, mother's maiden name, biometric data (fingerprints/voice print/retinal image/etc.), any other unique electronic identification number, and telecommunication access device, and violations may result in severe penalties, including jail time. It does not include publicly available information, but may include an individual's first name or first initial and last name in combination with one or more of the following items, if the name and the items are not encrypted:

Social Security number; Driver's license number, Credit/debit card number in combination with a password or security code OR information that identifies an individual and relates to the physical/mental health condition of the individual, the provision of health care to the individual; or payment for the provision of health care to the individual.

Businesses must have reasonable written policies and procedures to protect and maintain this private information. It is illegal to obtain, possess, transfer, or use this information without consent and with intent to obtain goods, services, insurance, credit, or any other thing of value in the other person's name.

Shredding paper files and properly eradicating electronic files must be done to ensure the PHI and financial information is completely unusable for any purposes.

Individuals must be notified if there is a breach of unencrypted information. The Texas Attorney General must be **notified of all data breaches affecting 250 or more Texas residents**; and, if a Covered Entity fails to comply with the breach notification requirements within 60 days, they can be fined $100 per individual, per day, up to a maximum of $250,000 per breach. (Please note: The HIPAA folks require notification within 60 days for breaches involving **500+** people.) Again, these penalties are additional to any imposed for non-compliance with the HIPAA Breach Notification Rule. If it's an electronic breach, the information must be disclosed as quickly as possible and affected individuals must be notified as soon as possible (law enforcement may require delaying notification so that it won't interfere with an investigation, but the notice should be made as soon as possible once permission is given). If a breach involves people outside the state of Texas, notification under the other state's rules is sufficient. However, any covered entity outside of Texas must comply with all notification rules for any private health information for Texas citizens or any private health information owned or stored within Texas.

If a breach/identity theft occurs, the entity may give notice in writing and/or verbally. (For a small office, for example, notification may be given over the phone and then followed up with a written or electronic notice). Quickly notifying

about a breach shows that the entity is trying to comply as soon as possible, but always check with your own attorney about what to do in the event of a breach/identity theft.

If someone's information is stolen, a district court can write an order saying that the person is a victim of identity theft and identify the individuals responsible for the offense.

If breaches resulting in identity theft are not reported as soon as possible to the attorney general's office, the attorney general can bring an action to recover a civil penalty or $100 per individual, per day that the entity fails to take reasonable action to comply with the notification rules, not to exceed $250,000 for a single breach. Attorneys' fees and costs may also be granted. Please note that the threshold to report a violation for a breach of any sensitive personal information is $250 under HB300. It's $500 for breaches of PHI that have to be reported to HIPAA immediately.