HB300

“Texas HIPAA”

Impact Date

September 1, 2012

HB 300 IMPACT

- Changes Texas Health and Safety Code
- Dramatically Impacts ALL Texans
- Massive Fines for Violations
- Attorney General Website to Report Violations
- Requires Annual Documented Training
- State to Seize Medical Records

New Training

"Covered entities" are mandated to train all employees on HB-300:
Within 60 days of hiring new employees.

Within 60 days after the effective date (Sept. 1, 2012) for existing employees.

Each employee must sign as attending, and records kept by covered entity.

Every 2 years thereafter

Key Definitions

Texas HB300 references Federal HIPAA terms, such as “protected health information,” “disclose,” and “covered entity,” and redefines them so broadly as to snare most Texans with draconian penalties for commonplace activities.

"Protected Health Information" TX HS. CODE ANN. § 182.002 : means protected health information as that term is defined by the privacy rule of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) contained in 45 C.F.R. Part 160* and 45 C.F.R. Part 164, Subparts A and E.*45 C.F.R. Part 160

*Protected health information means individually identifiable health information:(1) Except as provided in paragraph (2) of this definition, that is:(i) Transmitted by electronic media;(ii) Maintained in electronic media; or(iii) Transmitted or maintained in any other form or medium.(2) Protected health information excludes individually identifiable health information in:(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and(iii) Employment records held by a covered entity in its role as employer.

“Disclose” 181.001(b)(2-a) means to release, transfer, provide access to, or otherwise divulge information outside the entity holding the information.

“Health Information” means any information, whether oral or recorded in any form or medium, that: 1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

“Individually identifiable health information” is information that is a subset of health information, including demographic information collected from an individual, and:(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and(i) That identifies the individual; or(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

“Covered Entity”= YOU

- Hospitals
- Medical Providers
- EMS/Fire
- Schools
- Employees
- Churches
- Sports Teams
- Camps
- Ambulance
- Labs
- Imaging
- Doctors
- Tech Support
- Administrators
- Transportation
- Individuals

Negligent Release

If protected medical information is released without authorization, misdirected, stolen, or lost, the affected individual(s) must be informed on penalty of fines at $100/day/record and possible felony charges.

Electronic Release

- Post a sign that says Health Information may be released electronically.
- Must provide electronic medical records to individual within 15 days of written request, if EMR is capable. Data should be encrypted.
- Each disclosure or release of health information must have a signed permission document, <u>except</u>:
  - (c) The authorization for electronic disclosure of unprotected health information is <u>not required if the disclosure is made to another covered entity</u>, as that term is defined by Section 181.001, or to a covered entity, as that term is defined by Section 602.001, Insurance Code, for the purpose of (A) treatment(B) payment(C) health care operations; or (D) performing an insurance or health maintenance organization function described by Section 602.053,Insurance Code;or,(2) as otherwise authorized or required by state or federal law.

FAQ

Do I need a release to send a referral note?
NO, releases to other covered entities are specifically exempt.

Do patients have to sign another form?
NO, you may give notice of electronic release by placing a sign.

If my employee texts me protected health information is that a violation?
NO, employees are a covered entities, but use caution. A misdirected text would be a violation.

If a patient emails me a medical question can I answer?
STOP. GET separate written authorization from the patient for each electronic transmission or this would be a violation.

Will I need a signed release to file an insurance claim?
NO, this is specifically exempt.

Can I Facebook about an interesting case?
UNWISE. If someone identifies the person involved, you are a violator.

Will employees be fined if they release protected health information without authorization?
YES, under HB300 the individual violator is fined.

Business Associates

Amend contracts with suppliers, vendors and contractors who may contact PHI to include HB300 language.

Closing Office

As of September 1, 2012, a doctor retiring, closing a practice, or moving, is termed an “unsustainable covered entity.” The State of Texas intends to take possession of your medical records.

SECTION 19.

(a) In this section, "unsustainable covered entity" means a covered entity, as defined by Section 181.001, Health and Safety Code, that ceases to operate.
(b) The Health and Human Services Commission, in consultation with the Texas Health Services Authority and the Texas Medical Board, shall review issues regarding the security and accessibility of protected health information maintained by an unsustainable covered entity.
(c) Not later than December 1, 2012, the Health and Human Services Commission shall submit to the appropriate standing committees of the senate and the house of representatives recommendations for:

(1) the state agency to which the protected health information maintained by an unsustainable covered entity should be transferred for storage;
(2) ensuring the security of protected health information maintained by unsustainable covered entities in this state, including secure transfer methods from the covered entity to the state;
(3) the method and period of time for which protected health information should be maintained by the state after transfer from an unsustainable covered entity;
(4) methods and processes by which an individual should be able to access the individual's protected health information after transfer to the state; and
(5) funding for the storage of protected health information after transfer to the state.

Example 1

A laptop is stolen from an employee of a Business Associate (BA). The computer contained Protected Health Information (PHI) on 656 individuals. The PHI included names, social security numbers, dates of birth, and medications. In response, the office took steps to enforce the requirements of the Business Associate Agreement (BAA). The BA agreed to install encryption software on all their mobile devices, strengthen IT access controls, update security policies, and improve the physical security of their building. In addition, the responsible employee was counseled and all employees received additional security training.

HB 300 holds accountable anyone in Texas that comes into contact with PHI. This means that your BAs will be accountable to the provisions of HIPAA and HB 300 unless they have no contact with PHI. Revise BAAs to include language requiring BAs to comply with state and federal privacy rules. BAA should address:

Immediate notification when a breach is discovered;

Clarify who notifies affected individuals by mail, who incurs the cost;

Contract terminates if BA fails to comply with privacy laws or take "reasonable" steps to fix the breach;

Evidence that BA performs security risk analysis at least annually;

Evidence BA provides required privacy training to employees; and

Encrypt PHI on BA's mobile devices, when BA exchanges PHI online or where PHI is at risk.

Penalties...

HB 300 privacy protections will be enforced through financial penalties, disciplinary actions, and audits that are intended to deter breaches. A court may consider several factors when determining the consequence of a breach including:

1) seriousness of the violation;

2) the entity's compliance history;

3) harm done to individuals; and

4) efforts made to correct violations.

Civil penalties of $5,000- $1.5 Million* may be assessed...

A civil penalty assessed under this section may not exceed $3,000 for each violation

Example 2

An unencrypted USB drive used to store billing data including PHI goes missing from the office. The drive contained data on 1,105 individuals including names, addresses, birth dates, diagnosis codes, and Social Security numbers.

The office subsequently notified all affected individuals and the local media. The office also added technical safeguards of encryption for all PHI stored on mobile devices; added physical safeguards by keeping new portable devices locked in a secure safe in the doctor's private office or in a secure filing cabinet; added administrative safeguards by requiring annual retraining of staff; and required immediate retraining of cleaning staff. (1)

HB 300 privacy protections will be enforced through financial penalties, disciplinary actions, and audits that are intended to deter breaches. A court may consider several factors when determining the consequence of a breach including: 1) seriousness of the violation; 2) the entity's compliance history; 3) harm done to individuals; and 4) efforts made to correct violations.

Civil penalties from may still be assessed in this case. Because the fine for negligent release of protected health information is $3000 per patient, fines may reach $3,315,000.

Keep PHI encrypted if it is in a form that could be easily lost or stolen.

PENALTIES

- $3,000/violation if committed negligently;
- $25,000/violation if committed knowingly or intentionally;
- $250,000/violation if committed intentionally and PHI is used for financial gain; and
- $1.5 million if a "pattern of practice" found.
- EACH RELEASE IS A VIOLATION

Example 3

EMS worker texts a photo of of an MVC with note, “Saw this today,” to his girlfriend at the local Volunteer Fire Department, who has just completed HB300 training. She recognizes the car, and forwards it to her cousin whose’ roommate “Jim” was injured in the accident, asking, “Heard your roomate has two broken legs! Is Jim out of ICU yet?”

The cousin replies, “He is better, but please pass it on to church to keep him in their prayers.” The cousin also posts a request to “Pray for Jim Thompson, who was hurt in a car accident, and is in the hospital,” on Facebook. She puts a note in the “In Our Prayers” box at church with Jim’s name, and that he is recovering from an accident.

The pastor announces the prayer request to the congregation of 186 people. In the back of the room is a lawyer, who texts his secretary about Jim’s injuries, and asks her to contact him at the hospital regarding his legal representation.

Number of VIOLATIONS:
EMS worker, EMS Service, No violation unless information is identifiable $0
Fire Department, - Negligent Release x1 $5000 =$5000
Girlfriend at VFD, - Intentional Release x1 $25,000 = $25,000
Cousin, (reply, Facebook posting, Prayer Box) -Negligent Release x3 each $3000=$9000
Pastor - Negligent Release x 186 each $3000=$558,000
Lawyer - Intentional Release for Financial Gain x1 $250,000

Total fines $845,000

Action Plan

1. Revise employee privacy training materials and policies;

2. Revise policies on patients' access to their EHRs;

3. Update and Post Notice of Privacy Practices;

4. Revise business associate agreements;

5. Get written permission from patient before engaging in or responding to electronic communication.

5. Encrypt PHI stored on mobile devices; and

6. Encrypt PHI sent electronically

7. Social Media Are Career Killers; Use Caution.

Sign Sample

Required Posting under HB300, effective 9/1/12

Texas Health and Safety Code Sec. 181.154 Requires

NOTICE AND AUTHORIZATION FOR ELECTRONIC DISCLOSURE OF PROTECTED HEALTH INFORMATION;

(a) A covered entity shall provide notice to an individual for whom the covered entity creates or receives protected health information if the individual 's protected health information is subject to electronic disclosure. A covered entity may provide general notice by: (1) posting a written notice in the covered entity 's place of business;

(b) may not electronically disclose an individual 's protected health information to any person without a separate authorization from the individual or the individual 's legally authorized representative for each disclosure. An authorization for disclosure under this subsection may be made in written or electronic form or in oral form if it is documented in writing by the covered entity.

(c) The authorization for electronic disclosure of protected health information described by Subsection (b) is not required if the disclosure is made:

to another covered entity, as that term is defined by Section 181.001, or to a covered entity, as that term is defined by Section 602.001, Insurance Code, for the purpose of:

(A)treatment;
(B)payment;
(C)health care operations; or
(D)performing an insurance or health maintenance organization function described by Section 602.053, Insurance Code; or as otherwise authorized or required by state or federal law.

Acknowledgement of Training

I Name (print) _____ acknowledge that I have undergone training in Texas HB300 privacy laws this on (Date)_____

Signature _____

I Name (print) _____ acknowledge that I have undergone training in Texas HB300 privacy laws this on (Date)_____
Signature _____

I Name (print) _____ acknowledge that I have undergone training in Texas HB300 privacy laws this on (Date)_____
Signature _____

I Name (print) _____ acknowledge that I have undergone training in Texas HB300 privacy laws this on (Date)_____
Signature _____

End

Following pages contain notes, references to text of law

Terms

- Under the Federal HIPAA law, “covered entity” is limited and defined as:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Texas' Terms

HB 300 redefines "covered entity" in the State of Texas

TEX HS. CODE ANN. § 181.001

(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.

Federal HIPAA:“Protected Health Information”

Federal Law:

§ 160.103 Definitions

•*Protected health information* means individually identifiable health information: ((4) "Individually identifiable health information" means individually identifiable health information as that term is defined by the privacy rule of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) contained in 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.)

§ 160.103 Definitions: *Health information* means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a *health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; **and**

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

**Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.*

***Health Services Defined(5) surgical dressings, and splints, casts, and other devices used for reduction of fractures and dislocations;(6) durable medical equipment;(7) ambulance service where the use of other methods of transportation is contraindicated by the individual’s condition, but, subject to section 1395m(l)(14) of this title, only to the extent provided in regulations;*

Exemptions

- (2) Protected health information **excludes** individually identifiable health information in:

(i) **Education records** covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ie

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(3) For the purposes of this section the term “educational agency or institution” means any public or private agency or institution which is the recipient of funds under any applicable program.

(4)(A) For the purposes of this section, the term “education records” means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which—

(i) contain information directly related to a student; and

(ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

(B) The term “education records” does not include—

(i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

(ii) records maintained by a **law enforcement unit of the educational agency** or institution that were created by that law enforcement unit for the purpose of law enforcement;

(iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person’s capacity as an employee and are not available for use for any other purpose; or

(iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.and

(iii) **Employment records held by a covered entity in its role as employer.**

Fact Sheet

Texas House Bill 300In June of 2011, Texas House Bill 300 was passed unanimously by both houses of the Legislature and signed by Governor Rick Perry, placing stricter requirements on patient health privacy covered entities. Federal law defines “covered entities” as health plans, health care clearinghouses, and health care providers that transmit health information in electronic form.

However, HB 300 expands definition of covered entities to include any entity or individual that:

§ 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;§ Comes into possession of protected health information; and§ Obtains or stores protected health information Requirements for Covered Entities Regarding Access to and Use of Protected Health Information.

Exceeding HIPAA Privacy Rule requirements, the bill as passed places the following requirements on covered entities around protected health information (PHI):

§ Covered entities must provide customized employee training regarding the maintenance and protection of electronic PHI, set deadlines for completion, and maintain records of completion of said training. Training will be required every two years.§ Patients must be provided with electronic copies (unless the patient is willing to accept this in another form) of their health information within fifteen days of the patient’s written request for the records. This is stricter than HIPAA’s requirement of thirty days. § Covered entities are required to provide notice that their PHI is subject to electronic disclosure.§ A covered entity is prohibited from disclosing a patient’s PHI to any other person in exchange direct or indirect payment—however, covered entities may disclose a patient’s PHI to other covered entities for treatment, payment, health care operations, insurance or HMO functions, or as authorized or required by federal or state law.

§ 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, in accordance with federal law (if feasible).§ The Health and Human Services Commission, in consultation with the THSA and Texas Medical Board “shall review the security and accessibility of protected health information maintained by an unsustainable covered entity” and present recommendations by December of 2012—this includes recommending **which state agency to which PHI from an unsustainable covered entity should be transferred for storage**.§ The Attorney General must create 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. In the report, patient PHI must be de-identified.§ The THSA (the state-designated entity for health information exchange) is charged with the development of privacy and security standards for the electronic sharing of PHI. **Individuals must be informed of a breach of their PHI**—this is consistent with HITECH requirements—and failure to do so will result in **financial penalty** and **potential felony charges.** This pertains to **any** business handling PHI, **not just covered entities** as defined by statute.

§ The State of Texas will take possession of all medical records when the person or entity closes

§ The law will **take effect September 1, 2012.**

Who did this?

Bill:
HB 300
Legislative Session: 82(R)

Primary Author
Date Filed
Kolkhorst
02/14/2011

Joint Author
Date Signed On
Naishtat
03/23/2011

Coauthors (8)
Date Signed On
Flynn
04/07/2011
Laubenberg
05/06/2011
Legler
05/02/2011
Murphy
05/02/2011
Smith, Todd
05/02/2011
Torres
05/02/2011
Truitt
05/02/2011
Zedler
04/07/2011

Senate Sponsor:
Jane Nelson

SENATE RULES SUSPENDED(Posting Rules)On motion of Senator West, on behalf of Senator Nelson, and by unanimous consent, Senate Rule 11.10(a) and Senate Rule 11.18(a) were suspended in order that the Committee on Health and Human Services might meet and consider the following bills today:iiHBi13, HBi335, HBi300, HBi3387.

COMMITTEE SUBSTITUTEHOUSE BILL 300 ON SECOND READINGOn motion of Senator Nelson and by unanimous consent, the regular order ofbusiness was suspended to take up for consideration CSHB 300 at this time on itssecond reading:Tuesday, May 24, 2011 SENATE JOURNAL 3341CSHB 300, Relating to the privacy of protected health information; providingadministrative and civil penalties.The bill was read second time.

COMMITTEE SUBSTITUTEHOUSE BILL 300 ON THIRD READINGSenator Nelson moved that **Senate Rule 7.18 and the Constitutional Rule requiring bills to be read on three several days be suspended** and that CSHBi300 be placed on its third reading and final passage.The motion prevailed by the following vote: iiYeasi31, Naysi0.

Signed by the Governor
06/17/2011

What were they thinking?

Legislative Session: 82(R)

House Bill 300
House Author: Kolkhorst et al.
Effective: 9-1-12
Senate Sponsor: Nelson

House Bill 300 amends the Health and Safety Code to update provisions relating to compliance with the federal Health Insurance Portability and Accountability Act of 1996 and the privacy of protected health information. The bill updates provisions establishing the duties of the executive commissioner of the Health and Human Services Commission (HHSC) with regard to protected health information. The bill includes provisions relating to training required for employees of covered entities, consumer access to and use of protected health information, and a report by the attorney general regarding consumer complaints. The bill prohibits the sale of protected health information by a covered entity, with certain exceptions, sets out requirements relating to the electronic disclosure of certain protected health information, and requires the attorney general, not later than January 1, 2013, to adopt a standard authorization form for use in complying with those requirements. The bill raises and sets caps on the civil penalty that may be assessed against a covered entity for a violation of state medical records privacy laws based on certain standards of culpability and includes provisions relating to an action by the attorney general and the disciplinary powers of a licensing agency with regard toa violation of state medical records privacy laws.

House Bill 300 establishes the powers and duties of HHSC relating to audits of covered entities and requires HHSC and the Texas Department of Insurance (TDI), in consultation with the Texas Health Services Authority (THSA), to apply for and actively pursue available federal funding for enforcement of state medical records privacy laws.

House Bill 300 amends provisions of the Business & Commerce Code requiring a person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information to disclose any breach of system security to any state resident whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person and makes that requirement applicable also to a resident of another state that does not require such disclosure. The bill enhances the penalty for an offense of identity theft by electronic device if the information accessed, read, scanned, stored, or transferred was protected health information.

House Bill 300 amends the Government Code to require HHSC, in consultation with the Department of State Health Services, the Texas Medical Board, and TDI, to explore and evaluate new developments in safeguarding protected health information and to annually report to the legislature on those developments and recommendations for the implementation of safeguards within HHSC.

House Bill 300 amends the Insurance Code to require a covered entity, as defined by that code, to comply with state medical records privacy laws relating to prohibited acts and with the standards for electronic sharing of protected health information.

House Bill 300 requires HHSC, in consultation with TSHA and the Texas Medical Board, to review issues regarding the security and accessibility of protected health information maintained by an unsustainable covered entity and to submit a legislative report including certain recommendations regarding those issues not later than December 1, 2012. The bill creates a task force on health information technology and requires the attorney general, not later than December 1, 2012, to appoint the task force members and chair.