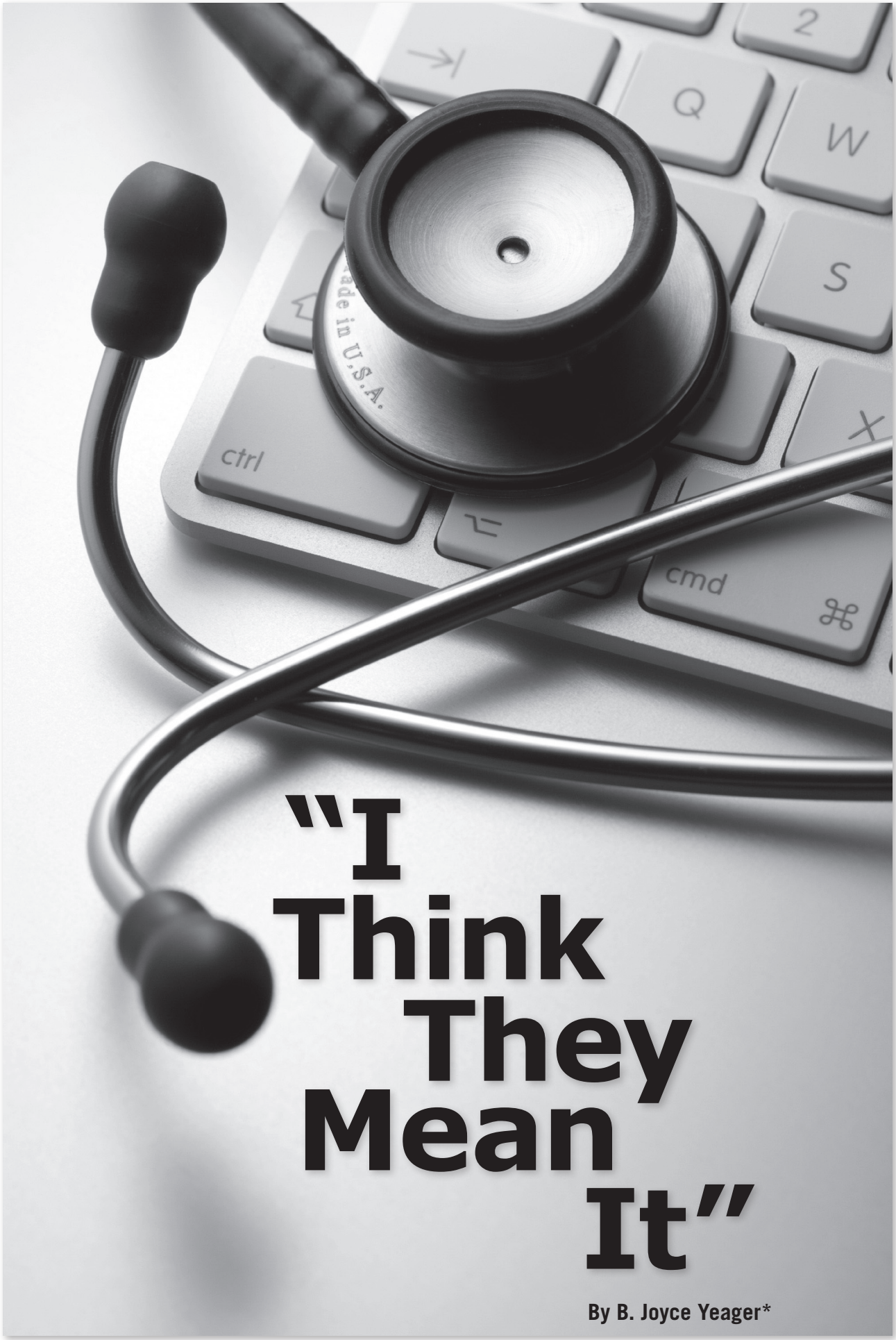

"I Think They Mean It"

By B. Joyce Yeager*

The New Medical Records Privacy Laws in Texas

A. Introduction

Revisions to the Texas Medical Records Privacy statute[1] which take effect on September 1, 2012, expand existing requirements for those who have access to medical information pertaining to others.[2] House Bill 300 (hereinafter, "HB 300" or "the Act") provides that covered entities, as defined in the statute, must comply with expanded responsibilities pertaining to health information.[3] The Act imposes upon these covered entities additional duties beyond those which are dictated by the federal Health Insurance Portability and Accountability Act of 1996 (hereinafter, "HIPAA").[4] Because the state statute affords additional protections beyond those provided by HIPAA, no federal preemption issue should exist.[5]

Penalties for failure to comply are substantial and include civil monetary penalties, the potential for loss of professional licensing, and even the potential for state law criminal felony prosecution. Entities and individuals within the State who have access to medical information of others have significant new responsibilities. It appears as though the legislature is serious about the protection of state residents' personal medical information and identifying demographics.

B. The Purpose of the Act? Protection

Expressing a concern for the potential for sale or unauthorized disclosure of personal health information, the legislature places tight restrictions on the manner in which patient data may be shared. The legislature noted:

> "Provisions of recent federal legislation establish incentives designed to increase the adoption of electronic health record systems among certain health care providers. The expanded use of such systems is likely to lead to the expansion of the electronic exchange of protected health information, which may require stronger state laws to better ensure the protection of that information. [H.B. 300] seeks to increase privacy and security protections for protected health information." [6]

In light of the concerns, the legislature mandates authorization before a provider may transfer patient data.[7] H.B. 300 is intended to provide Texans with significant additional protections beyond those provided by the federal HIPAA privacy, rule and Texas intends to be among the vanguard in health privacy regulation.[8]

The need for protection is obvious. One private, national study estimates that as many as 96 percent of all 72 health care providers which it surveyed indicate that they experienced a data breach in 2011, and that lost and stolen security devices and employee actions account for almost half of the breaches.[9]

C. The Statute's Elements, an Overview

C.1. What is Covered? What is PHI?

The Act defines an individual's protected health information, for a governmental entity, to include any information that reflects that an individual received health care from a covered entity that is not public information subject to disclosure by Chapter 552 of the Government Code.[10] For others, the definition of "protected health information" is engrafted from HIPAA.[11]

The Act incorporates the HIPAA provisions in effect as of September 1, 2011.[12] The Executive Commissioner of the Texas Health and Human Safety Commission is to determine whether it is in the best interest of the State to adopt any amendments made to these federal provisions which might be made at the federal level after September 1, 2011.[13] As defined in HIPAA, individually identifiable health information includes demographic data and health information created or received by a health care provider, a health plan, or health care clearinghouse which relates to:

1. An individual's past, present or future physical or mental health or condition;
2. The provision of health care to an individual;
3. The past, present or future payment for the provision of health care to the individual; and
4. The identity of the individual or with respect to which there is a reasonable basis to believe it can be used to identify the individual.[14]

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.[15]

HIPAA defines a health care provider as "a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[16] Protected health information, in turn, is defined as individually identifiable health information that is:

1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in *any other form or medium*.[17]

Excluded from this definition of protected health information is information within certain educational records and in employment records.[18]

Because the Act incorporates the provisions of HIPAA, a more thorough discussion of HIPAA is required for this article. This article will not directly address, however, provisions of related federal laws commonly referred to as HITECH, the American Recovery and Reinvestment Act of 2009 (AARA), Pub. L. No, 115-5, 123 Stat. 115, Health Information Technology for Economic and Clinical Health (HITECH Act), Sect. 13000, *et seq.* (Feb. 17, 2009). Detailed analysis of the HITECH provisions and the Act are beyond the scope of this overview article. For a discussion of HITECH and the Texas Privacy Laws, see, Patricia Gray, *Implementing Privacy and Security Standards in Electronic Health Information Exchange*,

University of Houston Health Law & Policy Institute, August 2011.

C.2. Who is covered? Who is a covered entity?

Section 181 in the Medical Records Privacy statute, will continue to define a "covered entity" to be *any person* who:

1. 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;
2. Comes into possession of protected health information;
3. Obtains or stores protected health information under the federal statute and regulations; or
4. Is an employee, agent, or contractor of one of these persons who creates, receives, obtains, maintains, uses, or transmits protected health information.[19]

This 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.[20] The Texas Medical Records Privacy statute, then, regulates anyone who comes into possession of personal health information ("PHI") or is an employee, agent, or contractor who creates, receives, obtains, maintains, uses, or transmits PHI. There are exemptions in the state act for:

1. Workers compensations plans and self-insured workers compensation plans;
2. Employee benefits plans;
3. Educational records covered by the Family Educational Rights and Privacy Act;[21]
4. Non-profits who pay for indigent medical care but have no medical primary purpose;
5. Processors of payment transactions in financial institutions; and
6. Handlers of criminal offenders with mental impairments.[22]

After the effective date of HB 300, also excluded from coverage of the Act will be those involved with crime victim compensation.[23]

C.3. What activities are restricted? Disclosure, sale.

C.3.1. Disclosure

It is important to note one key provision of the Act. The Texas statute contains one profoundly impactful, although seemingly innocuous, provision. The state statute defines the word "**disclose"** to mean any action to "release, transfer, provide access to, or otherwise divulge information outside the entity holding the information."[24] It is critical to fully absorb the impact of this definition. Anyone who transfers information, divulges information, or provides access to information must be aware of the implications for doing so without an authorization. Taken in its literal meaning, the definition of disclosure is so broad that it would encompass almost any activity whereby health information or demographics of others is involved. Any information about an individual's condition, care, payment, or identity is protected from being divulged or being accessed, no matter the form in which it might be maintained. Any covered entity, including associates of a covered entity, is affected by the statute in some manner. Exceptions are limited and the breadth of the statute's reach is staggering.

C.3.2. Sale of information

Of even greater significance is the Act's strict ban on the sale of protected health information. A covered entity may not disclose an individual's protected health information to any other person in exchange for direct or indirect remuneration.[25] Exceptions only allow disclosure to another covered entity under the statute or a covered entity under the Insurance Code for treatment, payment, health care operations, and insurance or certain HMO functions or as otherwise authorized or required by law. [26] Further, any charges for the disclosure for treatment, payment, health care operations, or to perform an insurance function cannot exceed the covered entity's reasonable costs in preparing and transmitting the PHI.[27]

Because the Act restricts *disclosure* of health information for even *indirect* remuneration, more than an outright ban on the sale of information is restricted. The Act restricts any transfer which results in even indirect financial gain which is not associated with treatment, payment, operations, insurance, or for compliance authorized by law or required by law.[28] The outright ban on disclosure for even indirect remuneration does not have any mechanism for allowing for disclosure, not even after notice and consent or authorization. Rather, the disclosure for remuneration is flatly banned. Because the Act would ban even indirect remuneration, it is possible that the Act would implicate, for example, social media interactions or advertising in the form of patient testimonials even if these are the result of patient consent or even the result of patient initiated activity.

The ability to engage in activities which might result in indirect remuneration with the consent or authorization of the owner of the information and to do so because those actions are protected constitutionally as, for example, free speech or commercial speech, is beyond the scope of this overview article. For discussion of such principles, s*ee*, *e.g.*, *Sorrell v. IMS Health, Inc.,* __ U.S. __, 131 S.Ct. 2653 (2011). In *Sorell*, the United States Supreme Court determined that restrictions on the sale, disclosure, and use of pharmacy records as attempted by implementation of Vermont's Prescription Confidentiality Law, Vt. Stat. Ann., Tit. 18, 4631(d), was unconstitutional because the statute, which imposed content-based and speaker-based burdens on protected expression, banned sales of the information to only some potential users.

D. What additional duties are imposed? Consumer Access, Notice, Training

D.1. Patient access to records

The Act provides that if a health care provider is using an electronic health care records system that is capable of fulfilling the request, the health care provider, no later than 15 business days following the written request for an electronic health care record, must provide the information electronically unless the person making the request agrees to accept the record in another form.[29] An exception is available for records exempt pursuant to 45 C.F.R. § 164.524 for specific types of records such as certain psychotherapy notes, information compiled for use in certain legal proceedings, and certain select laboratory records. [30]

The Executive Commissioner of Texas Health and Human Services, in consultation with the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance may recommend a standard electronic format, but any format recommended must be consistent with federal law regarding the release of medical records.[31] As of this writing, the Executive Commissioner's Office had not yet made a determination concerning the undertaking of this unenviable task.[32] There can be no doubt that the choice of the word "may" in the statute was an intentional one.

D.2. Notice and authorization requirements

Any covered entity that create and receive personal health information must provide notice to individuals if their personal health information is subject to electronic disclosure.[33] The duty to provide notice is, however, only a general one and the notice can be provided by:

1. Posting written notice in place of business; or
2. Posting notice on web site; or
3. Posting notice in place where individuals whose PHI is subject to electronic disclosure are likely to see the notice.[34]

According to Texas Health Services Authority General Counsel Jocelyn Dabeau, this notice must be conspicuous and understandable.[35]

Of greatest significance, perhaps, to medical practitioners, is the requirement that a covered entity may not electronically disclose an individual's protected heath information to *any* person without a separate *authorization* from the individual, or the individual's legally authorized representative, for *each* disclosure.[36] The authorization for electronic disclosure is not required, however, if the disclosure is made to another covered entity under the Act or to any covered entity as defined by Section 602.001 of the Insurance Code *solely* for purposes of treatment, payment, health care operations, if performing health maintenance organization functions as defined by the Insurance Code, or if otherwise authorized or required by state or federal law.[37] The authorization for this disclosure may be made in written form, in electronic form, or in oral form *if* the request is documented in writing by the covered entity.[38] The State Attorney General will adopt a standard form for use with obtaining authorizations and the form will also comply with the Health Insurance Portability and Accountability Act and Privacy Standards, if possible.[39] As of this writing, the State Attorney General did not yet have an anticipated release date but noted that Section 22 of the Act provides for a date of January 1, 2013.[40]

This author assumes that for any such oral authorization to be valid, it would require contemporaneous documentation of the request at the time it was made. As a practical matter, given the audit functions provided in the Act,[41] it would be a best practice to maintain a separate chart for all such patient HIPAA and state privacy law interactions, if possible. In addition, when orally accepting a request for disclosure or accepting a written request in person or electronically, it would be a best practice to again provide general notice about the electronic disclosures.

D.3. Training required

Covered entities must provide a training program on state and federal law pertaining to protected health information as it relates to the covered entity's particular course of business. Each employee must be trained, but only trained so as to function within their scope of employment.[42] This training must be completed within 60 days of employment and at least once every 2 years.[43] The covered entity shall require employees who attend training to sign an electronic or written statement verifying attendance at the training program, and the covered entity is to maintain the signed statement.

Unfortunately, the Act does not indicate that any governmental or educational entity will provide input into the content of any training programs or provide certification for those who will provide the training. However, as of September 15, 2011, no state agency was contemplating oversight of training programs.[44] The State Attorney General's Office is planning no such function.[45]

The Act does not provide a deadline for a covered entity to provide training for those employees who are already employed as of the effective date of the Act. However, given the mitigation available as to the potentially onerous penalties for non-compliance (*see*, herein, Section E, *infra*), a covered entity would be engaged in best practices if all employees were provided, at a minimum, training applicable to their job function as soon as practicable.

It can be logically assumed that less substantive training would be required for someone who merely filed a patient's paper chart onto the proper place on a shelf than would be required for someone who was responsible for the electronic transmission of records or someone who was responsible for the covered entity's privacy policies or administration.[46] However, anyone who has access to patient records or gains access to patient information is capable of disclosure or breach.[47] In the event that any resulting civil penalty could be mitigated by the existence of a training program (*see* discussion, *infra*), providing training to employees and requiring that vendors and business associates, and, particularly, those providing information technology services, also demonstrate compliance with training requirements would be very beneficial. In the event one finds himself or herself with a need, in the future, to argue for mitigation of any civil penalties to be imposed, the existence of evidence of uniform, substantive training will be helpful. In the event training is undertaken from within an organization, best practices would involve retaining records of the training content as well as those who were trained.

Anyone who has access to patient records or gains access to patient information is capable of disclosure or breach.

E. What are the penalties for non-compliance? Audits, monetary fines, felony criminal charges, loss of professional licenses

E.1. Audits

The Texas Health and Human Services Commission, in connection with the State Attorney General, the Texas Health Services Authority, and the Texas Department of Insurance, may request that the United States Secretary of Health and Human Services conduct an audit of a covered entity as to the compliance of the covered entity with HIPAA.[48] The Commission is also charged with periodic monitoring and review of the results of audits of covered entities from within the state which are conducted by the United States Secretary of Health and Human Services.[49] It is unclear what authority the federal auditors would have to monitor for state law violations or whether federal auditors would even be aware of state law violations, given that the state law requirements are more extensive than the federal. According to the U.S. Department of Health & Human Services, a pilot program of federal audits was scheduled to begin in November 2011, and the pilot is to be completed in December 2012.[50]

If the Texas Health and Human Services Commission becomes aware of egregious violations which demonstrate a pattern and practice, the Commission may require a covered entity to submit to the Commission any federal risk analysis which the covered entity prepares in order to comply with HIPAA.[51] In addition, if the covered entity is licensed by a state agency, the Commission may request the licensing agency to conduct an audit of the covered entity's system to determine compliance with the Act. [52]

A significant number of potentially overlapping regulatory schemes and enforcement authorities could be implicated by this requirement in the Act.[53] The Act does not require training for any state or federal agency enforcement personnel.

E.2. Civil Penalties for Non-compliance

In addition to the injunctive relief already available pursuant to the current Health and Safety Code Section 181.201(a), the State Attorney General may, after the effective date of the Act, institute an action for civil penalties for violations of the Act not to exceed:

1. $5,000 per violation per year if negligent;
2. $25,000 per violation per year if knowing or intentional, regardless of the length of time of the violation within the year; or
3. $250,000 for each violation if knowing or intentional and for financial gain.[54]

In the event an adjudicator finds that the violations have occurred with a frequency so as to constitute a pattern or practice, the total amount of any civil monetary penalty which the court may assess is not to exceed $1.5 million annually.[55]

A discussion of applicable definitions for the terms "negligence" or "knowing and intentional" is beyond the scope of this overview article. Language contained within the regulations applicable to the Social Security Act seem helpful in describing levels of culpability in civil administrative functions.[56] Penalties may be limited or mitigated, in the event the disclosure was made only to another covered entity for purposes of treatment, payment, health care operations, or performing functions of a health maintenance organization; if the information disclosed was encrypted or transmitted using encryption technology; or, if at the time of the disclosure, the covered entity had maintained proper procedures including implementation of security procedures and training.[57] Factors are also provided by the Act for determining the appropriate financial penalty and include:

1. The seriousness of the violation;
2. The entity's compliance history;
3. Whether the violation poses a significant risk of financial, reputational or other harm to the individual whose protected health information was involved in the violation;
4. Whether the covered entity was working with or as a certified entity, that is, certified to be in compliance with privacy and security standards being developed by the Texas Health Services Authority as per Section 182.108 of the Health and Safety Code for the electronic sharing of protected health information;
5. The amount necessary to deter future violations; and
6. The covered entity's efforts to correct the violation.[58]

It is this author's contention that one should not have to establish harm to the victim in such instances. To determine the financial penalty, adjudicators will consider, in the event of disclosure, both monetary and *non-monetary* losses.[59]

Non-monetary losses include humiliation, embarrassment, mental anguish, fear of social ostracism, and other severe emotional distress.[60] Non-monetary victim losses also include the increased risk that personal health facts will continue to be disclosed, the increased risk of identity theft, and the increased risk of medical identify theft.[61] Patients themselves express the concern that their data will be misused for commercial gain, that disclosure will result in embarrassment, that disclosure will compromise their personal safety, that their data will be used in a discriminatory fashion impacting their lives and care, that there will be no opportunity to correct any false information circulated, and that there will be loss of their data or loss of access to their data.[62]

Losses to a health care provider in the event of an unauthorized disclosure are also significant and include the costs associated with the potential loss of the economic value of a patient who no longer associates with an organization following a breach.[63] At least one study identifies the lifetime economic value, on average, of one patient or customer to fall within a range from $10,000 to over $1,000,000.[64]

In addition to civil penalties, a covered entity which is licensed by a state agency is subject to investigation and disciplinary proceedings, including probation or suspension by the licensing agency.[65] A license may be revoked if the violations are egregious and constitute a pattern and practice. The attorney general of the state may institute an action for violation of the Act against a covered entity that is licensed by a licensing agency of this state for a civil financial penalty only if the licensing agency refers the violation to the attorney general.[66]

F. What other resources will be available? Websites, Standards

F.1. Websites

The Texas Attorney General is to develop and provide a consumer information website which will include information on the manner in which to make a complaint.[67] As of this writing, the State Attorney General did not yet have an anticipated release date, but noted that Section 22 of the Act provides for a date of May 1, 2013.[68] The author notes that the Act becomes effective September 1, 2012. Certain materials are directed, by statute, to be included on the website.[69] The Texas Attorney General is also charged with monitoring consumer complaints and with reporting on the complaints after de-identifying the protected health information.[70]

F.2. Standards

The Texas Health Services Authority is tasked with rulemaking for the certification of entities undertaking the electronic exchange of protected health information.[71] The Texas Health Services Authority is to establish standards for the secure electronic exchange of protected health information.[72] The Authority must develop, and submit to the Health and Human Services Commission for ratification, the privacy and security standards for electronic sharing. The Authority is also tasked with developing voluntary operations and technical standards for health information exchanges in Texas.[73] Concern has been expressed by some concerning the *consent* options which will be required in health information exchanges when the Act's requirement is for *authorization* for the release of information.[74]

G. What Other State Statutes Are Amended or Affected? Breach notification laws, the Insurance Code

G.1. Breach notification

In HB 300, the legislature also expanded the state's breach notification requirements already existing in the Business and Commerce Code at Sections 521.053 and 521.151.[75] The expanded notification will require notice not only to state residents in the event of a breach, as previously required, but to *all* affected individuals.[76] Because notice is to be given to all individuals and not only state citizens, the reach of the statute in its regulation of any covered entity within the state will undoubtedly have nationwide or even global impact. The Dallas Regional Chamber of Commerce estimates the health care industry contributes $52 billion dollars annually to the Dallas–Fort Worth area alone, supporting an estimated 601,000 regional jobs and driving up to 15 percent of the area economy.[77] In addition to time and productivity losses in the event of a breach, the economic impacts identified in one study estimated costs for data breach incidents to hospitals being surveyed to be in a range from $10,000 to over $10,000,000 per entity in a two year period.[78]

Texas' Business Code already includes notice requirements for breaches of information pertaining to "personal identifying infor-

mation," identified in the Business Code breach notification provisions to include biometric data, the physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to the individual.[79] HB 300 added to the breach notification penalty provisions of Business and Commerce Code Section 521.151 the ability to recover additional civil penalties of up to $100 per day, per individual affected, for an unreasonable delay in notification or failed notification of a breach of data.[80] Although the breach statute does not incorporate the Act's definition of PHI, the definition employed in the Business Code breach statute is broad enough to include PHI.[81] Including enhanced fines for the failure to notify in the event of a breach within the Act, without revising the Business Code to include a revised definition of PHI, demonstrates the legislature's intent that the two statutes are to work in an interrelated fashion.

Offenses for the use of a scanning device or re-encoder to access, read, scan, store, or transfer information encoded on the magnetic strip of a payment card without the consent of an authorized user of the payment card and with intent to harm or defraud another were previously codified as a Class B misdemeanor under the Business & Commerce Code.[82] Now, however, if such an offense also involves protected health information, as defined by HIPAA, the offense is defined as a felony.[83] If an element of the crime was committed prior to September 1, 2012, the offense was committed prior to the effective date of the act.[84] It is worth noting again that payment processors at financial institutions are not covered entities, however.[85]

G.2. The Insurance Code

The State Insurance Code, Chapter 602, was amended by HB 300 to require those covered by Chapter 602 of the Insurance Code to comply with Chapter 181, the Medical Records Privacy statutory provisions.[86] Consequently, the Act now also pertains to insurance companies which are exempt from HIPAA,[87] including:

1. County mutual insurance companies;
2. Farm mutual insurance companies;
3. Fraternal benefit societies;
4. Group hospital service corporations;
5. Lloyd's plans;
6. Local mutual aid associations;
7. Mutual insurance companies;
8. Reciprocal or interinsurance exchanges;
9. Statewide mutual assessment companies;
10. Stipulated premium companies;
11. Health maintenance organizations; and
12. Insurance agents.[88]

These individuals and organizations must comply with Act's provisions when it becomes effective on September 1, 2012. The distinctions in the Insurance Code between "health information" and "nonpublic health information," defined by Section 602.001 of the Insurance Code, is beyond the scope of this overview article. Section 602.002 of the Insurance Code provides that this chapter of the insurance code does not apply to a covered entity that is required to comply with the standards governing the privacy of individually identifiable health information adopted by the United States Secretary of Health and Human Services under Section 262(a), Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d, *et seq.*). Section 602.003 of the Insurance Code indicates the chapter does not preempt or supersede state law in effect on July 1, 2002 that relates to the privacy of medical records, health information, or insurance information. Section 602.053 of the Insurance Code provides exceptions which allow a covered entity to disclose nonpublic personal health information to the extent that the disclosure is necessary to perform the specified insurance or health maintenance organization functions, as identified in that provision, on behalf of the covered entity. The definition of "health information" in the Insurance Code does not include age and gender.[89]

H. Do other privacy laws exist as well? Yes.

Other state statutes and common law principles are not implicated by the Act and are not subsumed by the Act's provisions, including the existing body of legal and ethical principles pertaining to patient privileges.[90] There are a myriad of additional privacy statutes and regulations which will not be subsumed within the Act.[91] There are other state statutes which contain restrictions on the disclosure of records currently applicable to a variety of health care facilities such as nursing facilities, rehabilitation facilities, surgery centers, and emergency rooms. Mental health professionals also have their own patient privilege laws and ethical codes, particularly as to psychotherapy notes from a patient which the professional feels that it would not be in the patient's best interest to disclose. HIV and AIDS records and records pertaining to other communicable diseases are also subject to their own distinct disclosure provisions. Genetic information is separately regulated, as are substance abuse records, certain health study records, occupational condition reporting, and records pertaining to minors, inmate records, and school records. Biometric identifiers, Medicaid, State Children's Health Insurance Program Beneficiaries, other government records containing health information, and peer review committee investigation records are all given separate treatment in Texas law as well. Some of these laws, unlike the Act, provide individuals with a cause of action for unauthorized disclosure.[92]

It is clear that attorney client privileges would apply as to disclosures

between an attorney and the attorney's own client. It seems far less clear that attorneys would not be considered a covered entity when handling the protected health information of others in other instances. The legislature clearly carved such exceptions where it thought them to applicable and the legal profession was not provided with an exception.[93]

I. Conclusion

The Texas Medical Records Privacy statute is indeed aggressive in its reach. Its penalty provisions, if and when enforced, will almost certainly be a solid deterrent to all except the most unscrupulous and most careless. It is unfortunate that the burdens of compliance could further exacerbate the already burdensome administrative overlay existing for those in the state who provide health care and related services. Given the enormity of the need for the protection of health information and patient demographics, however, state governments can do no less than take an aggressive approach to supplement federal law pertaining to medical privacy. The provisions of House Bill 300 could create enormous exposure to covered entities as well as licensed individuals and groups. It should follow, then, that associations and individuals will be highly motivated to comply with the Act and to protect personal health information. The legislature was clearly serious, and the citizens of the state now await to see whether enforcement will bare out legislative intent.

** Ms. Yeager is a licensed attorney and Certified Information Privacy Professional. She prepared this article while practicing law in Texas. Ms. Yeager is now an Assistant Attorney General for the Office of the Attorney General of Missouri. Ms. Yeager is also the founder of Amenable Though, LLC, an organization committed to education and the arts. She can be reached at* b.joyce.yeager@gmail.com. *This article was originally published in the International Association of Privacy Professionals' monthly member newsletter, The Privacy Advisor, and is reprinted here with permission.*

---

1 Texas Health and Safety Code, Chapter 181, § 181.001, *et seq.,* amendments effective September 1, 2012.

2 House Bill 300, enacted June 17, 2011, and codified at Health and Safety Code Sections 181.001, 181.004, 181.005, 181.006, 181.059, 181.101, 181.102, 181.103, 181.104, 181.153, 181.154, 181.201, 181.202, 181.205, 181.206, 181.207, 182.002, 182.108; Business and Commerce Code Sections 521.053, 521.151, 522.002; Government Code Section 531.0994; and Insurance Code Section 602.054. Available at http://www.legis.state.tx.us/tlodocs/82R/billtext/html/HB00300F.htm, last visited March 5, 2012. Hereinafter, "HB 300".

3 *See,* herein, Sections A through E, *infra*.

4 *Compare*, HB 300, *with,* Title II, Subtitle F, 42 U.S.C. § 1320d, *et seq*., Pub. L. No. 104-191; 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

5 *See*, *Brown v. Mortensen*, 253 P.3d 522 (Cal. 2011) (California Confidentiality of Medical Information Act, Cal. Civ.Code, § 56, *et seq*. not preempted by Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d *et seq*., and the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, *et seq*.). *See also*, Cynthia Marietta and Patricia Gray, *Medical Information Privacy in Texas*, University of Houston Health Law & Policy 11, page 45, fn. 271, fn. 272; Patricia Gray, *Implementing Privacy and Security Standards in Electronic Health Information Exchange*, University of Houston Health Law & Policy Institute, August 2011; *Preemption Analysis of Texas Laws Relating to the Privacy of Health Information & the Health Insurance Portability & Accountability Act & Privacy Rules (HIPAA)*, Report of the Office of the Attorney-General of Texas, November 1, 2004, available at www.oag.state.tx.us/notice/hipaa.pdf, last visited May 7, 2012 (analysis prior to enactment of HB 300).

6 Bill Analysis, Committee Report, C.S.H.B. 300, Naishtat Kolkhorst, available at http://www.legis.state.tx.us/tlodocs/82R/analysis/html/HB00300H.htm, last visited May 5, 2012.

7 HB 300 Initial House Research, Naishtat Kolkhort, May 2, 2011, available at http://www.capitol.state.tx.us/tlodocs/82R/analysis/pdf/HB00300H.pdf#navpanes=0, last visited May 5, 2012.

8 HB 300 Initial House Research, Naishtat Kolkhort, May 2, 2011, available at http://www.capitol.state.tx.us/tlodocs/82R/analysis/pdf/HB00300H.pdf#navpanes=0, last visited May 5, 2012; *See also*, legislative history available at http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=82R&Bill=HB300, last visited May 5, 2012. (California also has a health privacy state law which supplements the protections afforded by federal law. *See*, Confidentiality of Medical Information Act, Calif. Civ. Code, § 56 *et seq*.)

9 *Second Annual Benchmark Study on Patient Privacy and Data Security*, Ponemon Institute Research Report, Ponemon Institute, December 2011, pp. 1-3, 20, 22.

10 HB 300, Section 4, codified at Health and Safety Code § 181.006.

11 Health and Safety Code § 181.001(a) provides that terms which are not identified in the Act are to be defined as per HIPAA. *See also,* HB 300, Section 1, codified at Health and Safety Code § 181.001.

12 *Id*.; 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.

13 HB 300, Section 3, codified at Health and Safety Code § 181.005.

14 45 CFR § 160.103, revised as of October 1, 2007 and available at http://edocket.access.gpo.gov/cfr_2007/octqtr/45cfr160.103.htm, last visited March 2, 2012. (S*ee also*, California Civil Code §56-56.07, "'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.")

15 45 C.F.R. Sect. 160.103, revised as of October 1, 2007 and available at http://edocket.access.gpo.gov/cfr_2007/octqtr/45cfr160.103.htm, last visited March 2, 2012 (emphasis added).

16 45 C.F.R. § 160.103, revised as of October 1, 2007, available at http://edocket.access.gpo.gov/cfr_2007/octqtr/45cfr160.103.htm, last visited March 2, 2012.

17 45 C.F.R. Sect. 160.103, revised as of October 1, 2007 and available at http://edocket.access.gpo.gov/cfr_2007/octqtr/45cfr160.103.htm, last visited March 2, 2012 (emphasis added).

18 *Id*.

19 Health and Safety Code § 181.001(b)(2).

20 *Id.*

21 Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

22 Health and Safety Code § 181.051; see also Jocelyn Dabeau, International Association of Privacy Professionals Privacy

Academy, September 15, 2011, https://www.privacyassociation.org/events_and_programs/2011_iapp_privacy_academy, last visited March 5, 2012.
23 HB 300, Section 5, Codified at Health and Safety Code § 181.059.
24 HB 300, Section 1, codified at Health and Safety Code, § 181.001(b)(2-a).
25 HB 300, Section 7, codified at Health and Safety Code, §181.153(a).
26 HB 300, Section 7, codified at Health and Safety Code, §§ 181.153(a)(1) and (a)(2). *Compare*, Insurance Code §§ 602.001 and 602.002, as amended by the Act, *with*, Health and Safety Code § 181.015, as amended by the Act.
27 HB 300, Section 7, codified at Health and Safety Code § 181.153(b).
28 *Id.*
29 HB 300, Section 6, codified at Health and Safety Code § 181.102.
30 *See*, 45 C.F.R. § 164.524 http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=7c7d0776f660da26d642766386867e6d&rgn=div8&view=text&node=45:1.0.1.3.79.5.27.12&idno=45, last reviewed May 5, 2012.
31 HB 300, Section 6, codified at Health and Safety Code § 181.102.
32 *See*, notes of interview with Stephanie Goodman, Texas Health and Human Services Commission conducted March 2, 2012, interview notes on file with author.
33 HB 300, Section 7, codified at Health and Safety Code § 181.154.
34 HB 300, Section 7, codified at Health and Safety Code § 181.154(a).
35 Jocelyn Dabeau, International Association of Privacy Professionals Privacy Academy, September 15, 2011, available online at https://www.privacyassociation.org/events_and_programs/2011_iapp_privacy_academy, last visited March 5, 2012.
36 HB 300, Section 7, codified at Health and Safety Code § 181.154(b) (emphasis added).
37 HB 300, Section 7, codified at Health and Safety Code § 181.154(c) (emphasis added0.
38 HB 300, Section 7, codified at Health and Safety Code § 181.154(b).
39 HB 300, Section 7, codified at Health and Safety Code § 181.154(d).
40 *See*, Interview, Thomas Kelly, Office of the Texas Attorney General, Interview March 6, 2012, interview notes on file with the author. The author notes that the Act becomes effective September 1, 2012.
41 S*ee*, discussion *infra* concerning auditing requirements imposed by the Act.
42 HB 300, Section 6, codified at Health and Safety Code § 181.101(a).
43 HB 300, Section 6, codified at Health and Safety Code § 181.101(b).
44 Jocelyn Dabeau, General Counsel, Texas Health Services Authority, International Association of Privacy Professionals Privacy Academy, September 15, 2011, available on line at https://www.privacyassociation.org/events_and_programs/2011_iapp_privacy_academy, last visited March 5, 2012.
45 *See*, Interview, Thomas Kelly, Office of the Texas Attorney General, Interview March 6, 2012, interview notes on file with the author.
46 Jocelyn Dabeau, General Counsel, Texas Health Services Authority, International Association of Privacy Professionals Privacy Academy, September 15, 2011, available on line at https://www.privacyassociation.org/events_and_programs/2011_iapp_privacy_academy, last visited March 5, 2012.
47 *See*, discussion on breaches, *supra*. See also, *Second Benchmark Study in Patient Privacy & Data Security*, Ponemon Institute Research Report, Ponemon Institute, December 2011, pp. 3-6.
48 HB 300, Sect. 11, codified at Health and Safety Code 181.206(a).
49 *Id*.
50 See, *HIPAA Privacy & Security Audit Program*, available online at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html, last visited March 6, 2012.
51 HB 300, Section 11, codified at Health and Safety Code § 181.206(b).
52 HB 300, Section 11, codified at Health and Safety Code § 181.206.
53 For a discussion of the state laws impacting health information regulation, see Cynthia Marietta and Patricia Gray, *Medical Information Privacy in Texas*, University of Houston Health Law & Policy Institute, February 11, pp. 34-44 and accompanying footnotes. *See also*, discussion in Section H, *infra*.
54 HB 300, Section 8, codified at Health and Safety Code § 181.201(b).
55 HB 300, Section 8, codified at Health and Safety Code § 181.201(c).
56 *See*, 42 USC 1320d-5 (General penalty for failure to comply with requirements and standards).
57 HB 300, Section 8, codified at Health and Safety Code § 181.201(b-1).
58 HB 300, Section 8, codified at Health and Safety Code § 181.201(d).
59 *Id. (emphasis added.).*
60 *FAA v. Cooper, Concerning Emotional Injury as Harm Under the Privacy Act*, Electronic Privacy Information Center, available at http://epic.org/amicus/cooper/, last visited March 6, 2012.
61 *Second Annual Benchmark Study on Patient Privacy & Data Security*, Ponemon Institute Research Report, Ponemon Institute, pp. 15-16, December 2011.
62 Patricia Gray, *Implementing Privacy and Security Standards in Electronic Health Information Exchange,* University of Houston Health Law & Policy Institute, August 2011, p. 4. Patients are also concerned about the ability of organizations to accurately provide notification. *Id*.
63 *Second Annual Benchmark Study on Patient Privacy & Data Security*, Ponemon Institute Research Report, Ponemon Institute, p. 13, December 2011.
64 *Id*.
65 HB 300, Section 9, codified at Health and Safety Code § 181.202.
66 HB 300, Section 8, codified at Health and Safety Code § 181.201(e).
67 HB 300, Section 6, codified at Health and Safety Code § 181.103.
68 *See*, Interview, Thomas Kelly, Office of the Texas Attorney General, Interview March 6, 2012, interview notes on file with the author.
69 HB 300, Section 6, codified at Health and Safety Code § 181.103.
70 HB 300, Section 6, codified at Health and Safety Code § 181.104.
71 *See*, footnote 13, *supra* and footnotes 52 to 53, *infra.*
72 HB 300, Section 13, codified at Health and Safety Code § 182.108; HB 300, Sections 19 to 25.
73 *See,* Patricia Gray, Texas Human Health Services and Texas Health Services Authority and State Health Information Exchange Cooperative Agreement, *August 2011 Implementation*

Report, University of Houston, available at http://thsa.org/media/2272/privacy%20and%20security%20task%20force%20presentation_6-1-2011-1.ppt, last visited, March 7, 2012; *Texas Health Services Authority Privacy and Security Task Force, Presentation,* June 1, 2011, available online at http://thsa.org/media/2272/privacy%20and%20security%20task%20force%20presentation_6-1-2011-1.ppt, last visited March 6, 2012 (including discussion of HITRUST Alliance for health information exchanges).

74 *Id*. *See also*, Matt Murray, M.D., *Life in the Trenches*, International Association of Privacy Professionals Privacy Academy, September 15, 2011, available online at http://www.thsa.org/media/2951/consent%20options%20for%20hie%20in%20texas_june%202011.pdf, last visited March 6, 2012.

75 HB 300, Sections 14 and 15, codified at Business and Commerce Code §§ 521.053 and 521.151, respectively.

76 *Id*.

77 *The Health Care Impact, Assessing the scope and depth of the health care industry in Dallas-Ft. Worth*, Dallas Regional Chamber, March 2011, p. 4.

78 *Second Annual Benchmark Study on Patient Privacy & Data Security*, Ponemon Institute Research Report, Ponemon Institute, December 2011, pp. 11 and 14.

79 Business & Commerce Code, § 521.002.

80 HB 300, Section 15, codified at Business and Commerce Code, § 521.151(a-1).

81 *Compare*, Health and Safety Code § 181.001(b)(2), *with* Business and Commerce Code, § 521.151(a-1).

82 Business and Commerce Code § 522.022(b).

83 HB 300, Section 16 codified at Health & Commerce Code § 522.002(b).

84 HB 300, Section 26.

85 *See*, exemption discussion, *supra*.

86 HB 300, Section 18, codified as Insurance Code § 602.054 as amended effective September 1, 2012.

87 Insurance Code § 602.002.

88 Insurance Code §§ 602.001 and 602.002.

89 Insurance Code § 602.001(2).

90 Cynthia Marietta and Patricia Gray, *Medical Information Privacy in Texas,* University of Houston Health Law & Policy Institute, February 2011, pp. 34–36 and footnotes 156 to 186 therein. This report provides an overview of other state laws and ethics principles pertaining to medical information privacy in Texas. *Id.*, p. 34-43 and accompanying footnotes 156 to 258 therein.

91 *See, Id.*

92 *Id.* at pp. 43-45 and accompanying footnotes 259 to 273 therein.

93 See, discussion, *supra* on exemptions.