WHAT WE ALL NEED TO KNOW ABOUT HIPAA, HOUSE BILL 300 AND DATA SECURITY

HEATHER L. HUGHES, J.D., CHPC
U.S. LEGAL SUPPORT, INC.
363 North Sam Houston Parkway East, Suite 1200
Houston, Texas 77060
hhughes@uslegalsupport.com

SHERRI A. EVANS
sevans@koonsfuller.com

TAYLOR T. IMEL
taylor@koonsfuller.com
KOONSFULLER, P.C.
109 North Post Oak Lane, Suite 425
Houston, Texas 77024
(713) 789-5112 (Telephone)
(713) 789-5123 (facsimile)
www.koonsfuller.com

State Bar of Texas
42nd ANNUAL
ADVANCED FAMILY LAW COURSE
August 1-4, 2016
San Antonio

CHAPTER 10

Heather L. Hughes, J.D., CHPC
U.S. Legal Support, Inc.
363 North Sam Houston Parkway East, Suite 1200
Houston, Texas 77060
832-201-3877
hhughes@uslegalsupport.com

EDUCATION

B.S. in Psychology, Florida State University – 1991

J.D., South Texas College of Law – 1999

Certified in Healthcare Privacy Compliance - 2015

PROFESSIONAL ACTIVITIES

Heather L. Hughes has over twenty years' experience in healthcare compliance for both healthcare entities and a national consulting firm. She has been the HIPAA Privacy Officer for a large private healthcare company and for the past ten years she has been the HIPAA Privacy Officer for U.S. Legal Support, Inc., a national litigation support firm with 60 offices across the country. She oversees the required Technical, Administrative and Physical safeguards for the company, drafts and reviews business associate agreements for all vendors, provides training for all employees, responds to incidents and sits on the executive Privacy Committee of the company.

Heather has been conducting HIPAA Risk Assessments for law firms, insurance companies, physician insurance companies and healthcare providers for over six years. She also presents over 100 continuing legal education seminars per year on HIPAA, Texas HB 300, FIPA and Data Security to law firms, corporate legal departments and bar associations across the country.

NATIONAL SPEAKING ENGAGEMENTS

- Author/Speaker on *HIPAA, HB 300 and Data Security* at the State Bar of Texas General Practice, Solo and Small Firm Section 2016
- Author/Speaker on *HIPAA and Data Security* at the Arkansas Trucking Seminar, Arkansas – 2015
- Speaker/Panelist on *HIPAA Privacy* at the Claims and Litigation Management Annual Conference, San Antonio - 2013
- Author/Speaker on *HIPAA and HITECH* at the ALI-ABA program, *Third Electronic Discovery and Digital Evidence Practitioners' Workshop*, NY, NY – 2011
- Author/Speaker on *HIPAA Data Security* at ABA's *eDiscovery and Digital Evidence Committee, Second Intermediate to Advanced Practitioner's Workshop ,* San Francisco - 2011
- Author/Speaker on *HIPAA and HITECH and the Discovery Process* at the State Bar of Texas, Texas Health Law, Austin - 2009

SHERRI A. EVANS
KOONSFULLER, P.C.
109 North Post Oak Lane, Suite 425
Houston, Texas 77024
Telephone: 713-789-5112
Facsimile: 713-789-5123
sevans@koonsfuller.com

Licenses, Certification

Board Certified, Family Law, Texas Board of Legal Specialization, 1998
Licensed by Supreme Court of the State of Texas, 1993
Admitted to practice before the U.S. Court of Appeals, Fifth Circuit;
U.S. District Court, Southern and Eastern District of Texas

Education

J.D.- 1992, Tulane Law School, New Orleans, LA
B.B.A. (Finance) - 1987, University of Texas, Austin, TX
Kingwood High School - 1983

Honors

Named "Best Lawyers in America," 2012, 2013, 2014, 2015
Named "Texas Top 50 Women" by Texas Monthly Magazine, 2014
Named "Houston Top 100 Attorneys" by Texas Monthly Magazine, 2014
Named "Super Lawyer" by Texas Monthly Magazine, 2008-2014
Named one of Houston's Best Family Lawyers, H Magazine, 2006-2008
Named "Rising Star" by Texas Monthly Magazine, 2003 – 2005

Professional Affiliations

International Academy of Matrimonial Lawyers, Fellow
American Academy of Matrimonial Lawyers, Fellow
ABA Family Law Trial Institute (Faculty, 2004-2007)
Houston Family Law Trial Institute (Faculty, 2009-2015)
Texas Bar Foundation, Fellow
State Bar of Texas, Family Law Section
State Bar of Texas, Family Law Council (Immediate Past Chair)
State Bar of Texas, Family Law Council (Pro Bono Committee; Legislative Committee)
Texas Academy of Family Law Specialists (Board Member)
Gulf Coast Family Law Specialists (Board Member 2000-2007)
(Secretary 2001-02; Treasurer 2002-03; President-Elect 2003-04; President 2004-05)
Texas Family Law Foundation, Fellow
College of the State Bar of Texas
Houston Bar Association, Family Law Section

Publications/Speaking Engagements

Course Director
Family Law Technology
State Bar of Texas, 2012

Course Director

Advanced Family Law Seminar

State Bar of Texas, 2008

Course Director

Family Law of the Front Lines

University of Texas Law School, 2003-2009

I Love You, You're Perfect, Now Change, Family Law Technology, State Bar of Texas, 2014

There is No Business Like Family Law Business, Advanced Business Law Seminar, State Bar of Texas, 2014

There is No Business Like Family Law Business, New Frontiers in Marital Property, State Bar of Texas, 2014

Understanding Business Entities and Why It Matters, Advanced Family Law Seminar, State Bar of Texas, 2014

Drafting the Perfect Petition, Advance Family Law Drafting Course, State Bar of Texas, 2013

The Reconstituted Estate, Advanced Family Law Seminar, State Bar of Texas, 2013

The Reconstituted Estate, Marriage Dissolution Institute, State Bar of Texas, 2013

My Case Doesn't Fit Your Guidelines, Innovations: Breaking Boundaries in Custody Litigation, University of Texas Law School, 2013

The Reconstituted Estate, Advanced Family Law Seminar, State Bar of Texas, 2012

Valuing the Reconstituted Estate, Marriage Dissolution Institute, State Bar of Texas, 2012

27th Annual Trial Institute, Texas Academy of Family Law Specialists, 2012

More than Sex, Drugs and Rock n Roll, Innovations: Breaking Boundaries in Custody Litigation, University of Texas Law School, 2012

Business Entities, Advance Family Law Drafting Course, State Bar of Texas, 2011

Social Media and Family Law, Advanced Family Law Seminar, State Bar of Texas, 2011

How to Cross Examine a Valuation Expert, Family Law on the Front Lines, University of Texas Law School, 2011

Legislative Update, 11th Biennial Family Law Legislative Update, University of Texas Law School, 2011

Expert Witnesses: Pitfalls and Warnings Advanced Family Law Seminar, State Bar of Texas, 2010

Business Entities from a Family Law Perspective, Family Law on the Front Lines, University of Texas Law School, 2010

Top Ten Tips for Settling or Negotiating Conservatorship Disputes, State Bar of Texas Annual Meeting, 2010

Family Law Red Flags in the Electronic Age, AAML Mid-Year Meeting, 2010

Pleadings, Ultimate Trial Notebook, State Bar of Texas, 2009

Advanced Business Valuation, Advanced Family Law Seminar, State Bar of Texas, 2009

Legislative Update, 10th Biennial Family Law Legislative Update, University of Texas Law School, 2009

Business Valuation, and then some, Marriage Dissolution Institute, State Bar of Texas, 2009

Common Evidentiary Problems in Family Law, Marriage Dissolution Institute, State Bar of Texas, 2007
Securing and Enforcing the Property Award, Advanced Family Law Seminar, State Bar of Texas, 2006

Use of Forensic Accountants in Divorce, Marriage Dissolution Institute, State Bar of Texas, 2006

Discovery in Family Law Cases, How to Practice Family Law in Texas, Half Moon Seminars, 2004

Various Articles, Checklist Manual, Second Edition, State Bar of Texas, Family Law Section, 2003

Gathering, Organizing and Using Financial Information in Complex Property Cases, Texas Family Law Practice for Paralegals. Half Moon Seminars, 2003

Tracing, Expert Witness Manual, State Bar of Texas, Family Law Section, 2002

Identifying Marital Property Issues Upon Divorce, Family Law of the Front Lines, University of Texas Law School, 2002

Predicates, Presumptions, and Privileges, Advanced Family Law Seminar, State Bar of Texas, 2001

Taxation of Stock Options, Marriage Dissolution Institute, State Bar of Texas, 2001

Organizing the Trial Notebook, Ultimate Trial Notebook, State Bar of Texas, 2000

Trying the Complex Property Case, Family Law Practice Seminar, University of Houston Law Foundation, 2000, 2001, 2003

Securing and Enforcing the Property Award, Advanced Family Law Seminar, State Bar of Texas, 2000

Ethical Considerations, Marriage Dissolution Institute, State Bar of Texas, 2000

Property Forms You Never Knew Were in the Family Law Practice Manual, Advance Family Law Drafting Course State Bar of Texas, 1999

Retracing: Conflicting Rules of Tracing, New Frontiers in Marital Property, State Bar of Texas, 1999

Child Support: How to Establish it, Withhold it, and Draft Decrees so That it Will be Enforceable, Family Law Seminar
Houston Volunteer Lawyers Program, 1999

Bankruptcy and Divorce Revisited, Texas Marital Property Institute, University of Texas School of Law, 1997

Taylor Toombs Imel
Attorney and Counselor at Law
KoonsFuller, P.C.
109 North Post Oak Lane, Suite 425
Houston, Texas 77024
(713) 789-5112
taylor@koonsfuller.com

PRACTICE AREA

100% Family Law

LICENCES, CERTIFICATIONS

Licensed by the Supreme Court of the State of Texas, 2010

PROFESSIONAL EXPERIENCE

KoonsFuller, P.C. – Houston, TX
Attorney and Counselor at Law

DePlaza & O'Connor, Family Law – Plano, TX
Attorney and Counselor at Law

Diana S. Friedman, P.C., Family Law – Dallas, TX
Attorney and Counselor at Law

EDUCATION

SMU Dedman School of Law – Dallas, TX
Juris Doctor, May 2010
Dean's Scholarship Recipient

Wake Forest University – Winston Salem, NC
Bachelor of Arts in Spanish and Communication, May 2007
Women's Varsity Soccer Team, Full Athletic Scholarship

HONORS

Named one of Houston's Top Lawyers, H-Texas Magazine, 2015

PROFESSIONAL ACTIVITIES AND AFFILIATIONS

Member, College of the State Bar of Texas
Member, State Bar of Texas – Family Law Section
Member, Houston Bar Association – Family Law Section
Associate, Burta Rhoads Raborn Family Law American Inn of Court

PUBLICATIONS/SPEAKING ENGAGEMENTS

Co-Author, Speaker, *"Divorce Cases from Start to Finish: From Filing Through Trial (Discovery Guidelines, Case Management, and Your Role During Settlement and Trial)*
Institute for Paralegal Education (2016)

Co-Author, "*Everything You Need to Know or Do if There is an Entity or Trust in Your Divorce Case*"
Marriage Dissolution Institute – Ch. 16 (2016)

Co-Author, *"Temporary Orders on Borrowed Time"*
Advanced Family Law Course – Ch. 70 (2015)

Co-Author, "*I Love You, You're Perfect, Now Change"*
Family Law Technology 360 – Ch. 13 (2014)

Co-Author, *"There's No Business Like Family Law Business"*
12th Annual Advanced Business Law Course – Ch. 1.3 (2014)

Co-Author, "*There's No Business Like Family Law Business"*
19th Annual New Frontiers in Marital Property Law – Ch. 4 (2014)

Co-Author, "*Understanding Business Entities and Why It Matters"*
Advanced Family Law Course – Ch. 26 (2014)

Co-Author, "*60 Websites In 60 Minutes*"
Marriage Dissolution Institute – Ch. 19 (2014)

Co-Author, "*The In re Stephanie Lee Conundrum: Making and Enforcing Agreements in Family Law"*
Texas College for Judicial Studies (2014)

Co-Author, "*Possession and Access for Children Under Three"*
Advanced Family Law Course – Ch. 25 (2011)

TABLE OF CONTENTS

I. INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) has changed the face of medical privacy laws at both the federal and state level. In the two decades since HIPAA came into effect, compliance with the Act's regulations governing the maintenance, release, and use of protected health information has only become more stringent and costlier for entities handling protected health information with the advent of the Health Information Technology for Economic and Clinical Health ("HITECH") at the federal level and other data breach laws at the state level. While HIPAA regulations have always been a barrier for family law practitioners in obtaining medical or mental health records of a party to a suit, the enactment of House Bill 300, The Texas Medical Records Privacy Act, by the Texas Legislature in 2011 subjected family law firms to new privacy, confidentiality, and disclosure requirements and hefty penalties and fines for failing to abide by the same. Thus, your understanding of the heightened burden that is placed upon you to protect sensitive health information from unauthorized disclosure is essential to effectively representing your clients and shielding your firm from potential liability.

The goal of this paper is to not only provide you with an overview of the federal and state laws with which you must comply, but also to provide you with practice tips and tools for properly requesting, disclosing, safeguarding, and preventing the wrongful dissemination of protected health information obtained during a case.

II. ACKNOWLEDGMENT

The authors want to acknowledge the work of Sarah Darnell at KoonsFuller, P.C, and Charles E. Hardy and Ann W. Jamieson of Higdon, Hardy & Zuflacht, L.L.P., in their *Texas HIPAA Guide for Lawyers* prepared for the Family Law Section of the San Antonio Bar Association and thank them for allowing us to use their article in drafting this paper.

III. OVERVIEW OF FEDRAL RULES AND REGULATIONS

A. HIPAA: The Privacy and Security Rules

1. Generally

The Health Insurance Portability and Accountability Act (HIPAA) can be found in 40 C.F.R. § 164.512 and was enacted in 1996 to, in pertinent part, address privacy and security concerns with the general disclosure and use of protected health information. The Act itself required the Secretary of the Department of Health and Human Services to issue privacy regulations if Congress did not enact privacy legislation within three years following enactment. As a result, at the end of 2000, the Department published what is now commonly known as the "Privacy Rule", establishing national standards for the use and disclosure of protected health information.[1] However, the Privacy Rule is a federal "floor" for patient protections and industry standards, and therefore the states maintain the ability to enforce their laws which exceed those provided by this Rule.

2. Who and What is Covered?

The Privacy Rule defines entities bound by the privacy standards as "covered entities", which include health plans, healthcare clearinghouses, and healthcare providers who conduct certain financial and administrative transactions electronically.[2] Additionally, business associates of those entities – meaning any person or organization that performs certain functions or activities on behalf of a covered entity that involve the use or disclosure of protected health information – are also subject to the regulations established by the Privacy Rule. Under the Privacy Rule, protected health information is considered all "individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."[3] The Privacy Rule further defines individually identifiable information as any demographic data relating to an individual's physical or mental health, whether past, present or future. Note, this includes many common individual identifiers that our clients have on various documents such as names, addresses, birth dates, and social security numbers.[4]

3. Uses and Disclosures

The Privacy Rule distinguishes between required disclosures and permitted and authorized uses and

[1] *See* Department of Health and Human Services, *Summary of the HIPAA Privacy Rule*, available at http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.

[2] *Id.*

[3] *Id.*

[4] *Id.*

disclosures of protected health information. For purposes of this paper, however, we will focus on permitted and authorized uses and disclosures.

Under the Privacy Rule, a covered entity is permitted to use and disclose protected health information, without a specific authorization from the individual whose information is to be disclosed, for the following purposes: (1) to the individual; (2) for treatment, payment, and health care operations; (3) where the individual has an opportunity to agree or object; (4) an incident to an otherwise permitted use and disclosure (5) public interest and benefit activities, including pursuant to other statues, regulations, or court orders; and (6) for purposes of research, public health, or health care operations. If none of these situations apply, a covered entity must obtain the individual's written authorization prior to any use or disclosure of that individual's protected health information. The authorization must contain specific information regarding (1) the information to be disclosed or used; (2) the persons and/or entities disclosing and receiving the information; (3) an expiration date for the authorization; (4) a statement regarding the individual's right to revoke the authorization in writing; (5) and the signature of the individual, along with the date of the signature. If the information sought includes psychotherapy notes, the same must be specifically included in the authorization, otherwise the psychotherapy notes cannot be disclosed.[5]

The Privacy Rule further establishes that a covered entity must make reasonable efforts to use and disclose only the minimum amount of protected health information needed to comply with the request. However, this requirement is not imposed in the following situations: (1) disclosure to the individual or the individual's representative; (2) disclosure to or a request by a health care provider for treatment; (3) use or disclosure pursuant to an authorization; (4) use or disclosure required by law; (5) disclosure for complaint investigation, compliance review or enforcement of this Rule; and (6) use or disclosure required for compliance with certain HIPAA rules.[6]

4. The Security Rule

The Security Rule, enacted in 2003, expanded the Privacy Rule by establishing national standards for protecting electronic protected health information.[7] The goal of the Security Rule is to allow covered entities to continually adopt new technology to improve the quality and efficiency of patient care, while also providing a mechanism to protect that information in the technological world. Essentially, the Security Rule established a subset of information to be covered by the Privacy Rule, that information being any "identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form".[8]

Pursuant to the Security Rule, covered entities must establish internal mechanisms and procedures for protecting and securing personal/sensitive information. Additionally, those covered entities must ensure that their business associates are likewise in compliance. Required safeguards, both physical and technical, include the following: (1) disaster recovery plans, malware protection, and firewalls; (2) accountability and maintenance records of hardware and electronic media used to store protected health information; (3) data back-up and storage; (4) unique user identification, auto log-off and password protection on all devices used to access company information (including email); (5) encryption of laptops, flash-drives and CDs containing medical or sensitive information; and (6) training for all employees on privacy and security.[9]

B. HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009 to provide an enforcement mechanism for the Privacy and Security Rules by imposing civil monetary penalties for HIPAA violations. Pursuant to HITECH, covered entities and their business associates are required to notify individuals and the Department of Health and Human Services of any security breach of protected health information. A breach is defined under HIPAA as "the acquisition, access, use or disclosure of protected health information in a manner not permitted . . . which compromises the security or privacy of the protected health information."[10] Covered entities may be subjected to civil penalties for the breaches ranging from $100 to $50,000 per violation, based upon the varying degrees of culpability of the covered entity, up to a maximum penalty of $1.5 million dollars for all violations of the same provision occurring in the same calendar year.[11] HITECH also gave State Attorneys

[5] *Id*.
[6] *Id*.
[7] *See* Department of Health and Human Services, *The Security Rule*, available at http://www.hhs.gov/hipaa/for-professionals/security/.
[8] *Id*.
[9] 45 C.F.R. §164.308
[10] 45 C.F.R. §164.402.
[11] *See* Department of Health and Human Services, *HITECH Act Enforcement Interim Final Rule*, available at http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html .

General the authority to bring civil actions on behalf of the residents of their respective states for violations of the HIPAA Privacy and Security Rules and to obtain damages on behalf of the residents.[12]

C. Enforcement by the Office for Civil Rights

The Office for Civil Rights of the Department of Health and Human Services has been tasked with enforcing HIPAA Privacy and Security Rules. As part of that duty, OCR conducts periodic audits of covered entities and business associates.[13] In addition, OCR investigates claims that are filed with the organization about a covered entity's failure to protect the privacy of health information. To investigate the claim, the following conditions must be apparent from the complaint: (1) the alleged breach must have taken place after the Rules took effect; (2) the complaint must be filed against a covered entity; (3) the complaint must allege an activity that, if proven true, would violate the Privacy or Security Rule; and (4) the complaint must have been filed within 180 days of knowledge of the alleged violation, absent good cause shown for the delay.[14] If a complaint is accepted for investigation, OCR notifies the person making the complaint and the covered entity, who are then asked to present information about the incident described in the complaint. If an investigation is launched, the covered entity named in the complaint is required by law to cooperate with the investigations.[15]

If OCR determines that a covered entity has been noncompliant with the Privacy or Security Rules, OCR can levy civil monetary penalties on the entity. [16] The amount to be levied depends on a variety of factors outlined in Section 160.408 and whether the noncompliance was due to "willful neglect".[17] However, the general rule is that a civil penalty shall be imposed on the covered entity if it is found responsible for a violation.[18] The following sanctions can be levied for each violation of the Privacy or Security Rules:

(1) not less than $100 but not more than $50,000, if the entity did not have knowledge and would not have knowledge by exercising due diligence;

(2) not less than $1,000 but not more than $50,000, if the violation was not due to willful negligence;

(3) not less than $10,000 but not more than $50,000, if the violation was due to willful neglect but was corrected within 30 days; or

(4) not less than $50,000 if the violation was due to willful neglect and was not corrected within 30 days.[19]

The sanctions are also capped at $1.5 million for violations of the same provision occurring within one year.[20] For more egregious violations, such as the selling of protected health information, the Department of Justice can levy a criminal sanction and impose jail time for up to ten years.

If a penalty is assessed, a notice must be sent to the covered entity as well as the complainant setting forth: (1) the statutory basis for the penalty; (2) a description of the findings and reasons the violations on the part of the covered entity subjected it to a penalty; (3) the amount levied, with a specific reference to Section 164.404; (4) any circumstances under Section 164.808 that may apply; and (5) instructions for a response to the notice.[21] Within 90 days of the notice, the covered entity may request a hearing before an administrative judge.[22] If no hearing is requested or the challenge to the penalty is denied, the collection of the sanction levied can be sought through civil action. OCR may also notify the attorney general of the state where the entity is located of the entity's violation to enforce the same.[23]

As of May 31, 2016, over 130,000 complaints have been received by OCR regarding noncompliance with the Privacy or Security Rules. Of those complaints, OCR has investigated and resolved over 24,000 cases, netting a total dollar amount of $36,639,200.00 in civil penalties. Most of the cases investigated by OCR have

[12] *See* Department of Health and Human Services, *State Attorneys General*, available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html.

[13] *See* Department of Health and Human Services, *How OCR Enforces HIPAA Privacy and Security Rules*, available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html.

[14] *See* Department of Health and Human Services, *What OCR Considers During Intake and Review*, available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/what-OCR-considers-during-intake-and-review/index.html.

[15] *See* Department of Health and Human Services, *How OCR Enforces HIPAA Privacy and Security Rules*, available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html.

[16] 45 C.F.R. §160.404.

[17] *Id* .

[18] 45 C.F.R. §160.402.

[19] 45 C.F.R. §160.404.

[20] *Id*.

[21] 45 C.F.R. §164.420

[22] *Id*.

[23] 45 C.F.R. §§160.422, 160.424, 160.426

dealt with impermissible uses and disclosures of protected health information.[24]

IV. STATE-IMPLEMENTED DATA BREACH NOTIFICATION LAWS

A. Generally

As stated above, the Privacy and Security Rules represent the federal "floor" for patient protection and industry standards. Many states, 47 to be exact, have now implemented date breach notification laws that are much broader in terms of the entities covered by the law and stricter than the regulations imposed by HIPAA and HITECH. Specifically, these state-imposed data breach laws require businesses and law firms to maintain the security of personal/sensitive information. Depending on the state, this can include credit card information, tax information, social security numbers, driver's license numbers, and other types of personal information obtained by laws firms and corporations during the regular course of business. Jurisdiction is not only housed in the state where the business or firm is located, but also where the individual whose personal information has been obtained by the law firm or corporation resides.

All 47 states who have implemented these laws require law firms and businesses to notify the individual of a breach of security of his or her personal/sensitive information, some even requiring notification to credit reporting agencies and the attorney general. Sixteen (16) states now allow for a private cause of action for Data Breach Notification violations, some under the state's unfair or deceptive trade practices act and some under the state's consumer protecting act.

B. HB 300: The Texas Medical Records Privacy Act

1. Purpose

In 2011, the Texas Legislature adopted House Bill 300, which amended the Texas Medical Records Privacy Act of the Texas Health and Safety Code to expand the definition of a covered entity under Texas law, impose new regulations for safeguarding protected health information and create harsher sanctions for violating the Act's provisions. The bill itself became effective on September 1, 2012.

2. Who is Covered?

The Texas Health and Safety Code defines covered entities as any individual, business or organization that: (1) engages 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; or (4) is an employee, agent, or contractor of a person or entity described above if the create, receive, obtain, maintain, use or transmit protected health information.[25] While HITECH only covers law firms representing covered entities, HB 300 has expounded upon those regulations to cover any law firm handling medical records, health insurance records, or healthcare billing records. This means that when you, as a family law practitioner, come into contact with protected health information, whether from your client, the opposing party, or a third party, you become subject to the rules and regulations established by HB 300.

3. What are the Requirements?

Since HB 300 mandates that lawyers shall follow the regulations set forth by HB 300, HIPAA, and HITECH, it is vital to understand those requirements in detail.

a. Employee Training

Covered entities must now provide ongoing, customized training on both the federal and state laws for employees within 90 days of hire and then again if the federal or state laws concerning protected health information change. Each employee must also sign a statement verifying his or her attendance and completion of the required training.[26]

b. Furnishing Copies of Electronic Health Records

Within 15 days of a request by the individual, covered entities must provide a record in electronic form to the individual.[27]

c. Duty to Provide Notice

[24] *See* Department of Health and Human Services, *Enforcement Highlights*, available at http://hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[25] *See* TEX. HEALTH & SAFETY CODE §181.101

[26] *Id.*

[27] *See* TEX. HEALTH & SAFETY CODE §181.102

Covered entities must also provide notice to individuals that their protected health information may be transmitted electronically. This duty to provide notice is a general one and can be done in writing in your law firm, may be posted on your website or may be posted where the clients are likely to see it.[28]

d. Breach Notification

Covered entities must also notify an individual if a breach of that individual's sensitive personal information, including that individual's protected health information, has occurred, meaning if that information was acquired or reasonably believed to have been acquired by an unauthorized person. Although HB 300 does not specifically define "sensitive personal information", it incorporates the definition set forth in Section 521.002 of the Texas Business and Commerce Code and thus includes:

(1) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(a) Social Security number;
(b) Driver's license number or government-issued identification number; or
(c) Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(2) information that identifies an individual and relates to:

(a) the physical or mental health or condition of the individual;
(b) the provision of health care to the individual; or
(c) payment for the provision of health care to the individual.

This means that documents that you handle on a daily basis, such as initial client information sheets, tax returns, bank statements, etc. may fall under the umbrella of sensitive information that must be safeguarded pursuant to HB 300.

e. Authorization for Disclosure of Information

As under HIPAA, HB 300 mandates that protected health information may not be disclosed without a HIPAA compliant authorization from the person from whom protected health information is requested, except in certain instances.[29] Disclosure is defined as a release, transfer, or providing access to, or otherwise divulging information outside of the entity holding the information.[30] However, a covered entity may disclose protected health information without an authorization provided that the disclosure is made to another covered entity and so long as the disclosure is made for the purpose of treatment, payment of a claim, health care operations, performance of an HMO function, or as otherwise permitted by state or federal law.[31]

At minimum, the written authorization must meet the following requirements: (1) be in writing; (2) be dated and signed by the patient or the patient's legal representative; (3) identify the information to be disclosed; (4) identify the person(s) or entity(ies) to which the information may be disclosed; and (5) may not be contained in the same document as the patient's consent to medical treatment.[32] It is also advisable to include an expiration date for the authorization; otherwise, the authorization will only be valid for 180 days from the signing of the same.[33] The Attorney General has adopted a uniform authorization that can be downloaded from the Attorney General's website.

4. What are the Penalties for a Violation of HB 300?

Pursuant to Section 181.201 of the Texas Health & Safety Code, the Attorney General may bring a suit on behalf on an individual whose health insurance information has been wrongfully disclosed and seek injunctive relief to restrain further violations of Chapter 181. Like HIPAA and HITECH, the civil penalties for an unauthorized disclosure of protected health information under HB 300 range in severity depending on the extent and the motivation behind the disclosure. Specifically, civil penalties range as follows: (1) $5,000 for each negligent violation within one year; (2) $25,000 for each knowing or intentional violation within one year; and (3) $250,000 for each violation where protected health information is used for financial gain. If the violations are found to constitute a "pattern or

[28] *See* TEX. HEALTH & SAFETY CODE §181.154
[29] TEX. HEALTH & SAFETY CODE §181.154(c).
[30] TEX. HEALTH & SAFETY CODE §181.002(2-a).
[31] TEX. HEALTH & SAFETY CODE §181.154(c)(1)-(2).
[32] TEX. HEALTH & SAFETY CODE §241.152(b).
[33] TEX. HEALTH & SAFETY CODE §241.152(c).

practice", then a penalty can be levied up to $1.5 million annually.[34]

In addition to monetary sanctions, the state can also subject the violating entity to disciplinary action, including probation and suspension by the licensing agency.[35] The covered entity may, however, introduce evidence of its good faith efforts to correct and mitigate the damage caused by the breach so as to avoid the imposition of the penalties.[36] Other factors that the state will consider when imposing sanctions are: (1) the severity of the violation; (2) the compliance history of the violating entity; (3) whether the violation poses a significant financial, reputational, or other risk to the individual; (4) whether the entity was in compliance with the state laws and certified under 182.108; and (5) the amount necessary to deter future violations.[37]

5. What Other Actions May be Taken by the State?

The Attorney General is also authorized by HB 300 to work in tandem with OCR and the Texas Department of Insurance in conducting audits of a covered entity and to monitor the results of that audit.[38] While certainly the focus seems to be on covered entities within the health care industry, law firms should already be taking appropriate measures to ensure compliance with the requirements set forth by HB 300 in the event of an audit or a complaint lodged against the firm.

V. TIPS FOR ENSURING COMPLIANCE WITH FEDERAL AND TEXAS LAWS

Now that you know that you are a covered entity, what do you need to do to protect yourself and your practice?

A. Begin Employee Training Now (if you haven't already)!

As discussed supra, HB 300 requires office training for each employee within 90 days from the date of hire. Obviously, those 90 days have likely passed for most employees at your firm. However, it is essential that those employees attend and complete requisite training on the privacy and security of protected health information as soon as practicable for your firm to be in compliance with Texas law. At a bare minimum, the training session(s) should discuss security and access to protected health information, proper disclosure and use of protected health information, and how to properly request protected health information from third parties. Likewise, employees need to understand the importance of encrypting and password protecting their clients' health information. Optimally, access to this information should be limited to solely those employees working on that particular case/client. Remember, all of your employees will need to sign an acknowledgement/verification evidencing their attendance and completion of the training. Make sure that you maintain a copy of that authorization for a period of at least six years from the date of signing, as the same is required by HB 300.

B. Implement Appropriate Security Measures

Although HB 300 does not specifically address the requisite security measures set forth in the Privacy and Security Rules, it is reasonable to assume that the Bill expanded the application of those security measures to the more broadly defined covered entities, meaning you. Therefore, it is essential that you begin implementing appropriate security measures to protect sensitive and personal information.

It is particularly important to ensure any and all medical and mental health records received by your office be encrypted and/or placed under lock and key to prevent their unauthorized use and disclosure. Additionally, all electronic devices storing the protected health information must likewise be encrypted and password protected and must include timeouts for non-use. This includes computers, flash drives, phones, tablets, CDs, etc. If you house medical records and other files in a particular location in the office, consider incorporating video security to enhance your client's privacy.

Email should also be encrypted to prevent unlawful disclosure of protected health information. It is not sufficient simply to encrypt the email connections – the email itself and the archived emails must be encrypted as well. However, it is probably best to avoid sending medical records via email to protect the individual's privacy and prevent unintentional disclosure to unauthorized third parties.

Finally, your office may use Dropbox and other storage devices for sharing large files both interoffice and with the opposing side. Be careful using these hosting services as they too have security issues. Make sure that any website you use to transmit documents that contain sensitive information is HIPAA compliant and

[34] TEX. HEALTH & SAFETY CODE §§181.201(b)(1)-(3) and 181.201(d)(1)-(6).
[35] TEX. HEALTH & SAFETY CODE §§181.202
[36] TEX. HEALTH & SAFETY CODE §§181.205(a)(1)-(2).
[37] TEX. HEALTH & SAFETY CODE §§181.205(b)(1)-(6).
[38] TEX. HEALTH & SAFETY CODE §§181.206(a)(1)-(2).

provides enhanced security measures such as encryption.

C. Always Get Your Client's Authorization

If you anticipate that your client's medical or mental health will be an issue in the case, go ahead and ask your client to sign and execute HIPAA releases authorizing you to receive and disclose his or her mental records to the opposing counsel, the court, and any experts that may be involved in the case. Additionally, if you intend on using protected health information as an exhibit in a deposition, you will likewise need to get your client's authorization to disclose that information during the course of the deposition. Remember, prior to releasing any of your client's medical or mental health records, you must ensure that the release is HIPAA and HB 300 compliant, as set forth above. Keep in mind that a separate authorization will need to be executed by your client for each healthcare provider from whom records are requested to be released. The execution of these releases not only protects your client from unauthorized disclosure, but protects your firm from any future suit for releasing your client's protected health information in the event the case and/or the attorney-client relationship go south.

D. Tailor Requests for Protected Health Information

Carefully consider and evaluate the issues involved in your case prior to requesting physical and/or mental health care records from your client, the other side or a third party. If the information will not be useful, then do not request it. There is simply no need to trigger your heightened burden under HB 300 for protecting the health information if the same will not likely be used during the pendency of the case. If, however, you determine that the health information is necessary, decide what specific health information is needed and only request the release of that specific information.

1. Include HIPAA Compliant Authorizations

It is likewise prudent to send an authorization for the release and disclosure of the protected health information to the opposing party when requesting the production of that party's medical and/or mental health records. If the party refuses to sign the authorization and release his or her records, you will likely need to file a Motion to Compel and ask the Court to overrule the other side's objections and assertions of privilege. Consider also asking the Court to require the other party to execute the authorization or issue an order compelling the health care provider to release the information.

2. Draft Valid Subpoenas for Medical and Mental Health Care Records

Once you have received a valid authorization or court order for the release of certain medical and/or mental health care records, you should issue a subpoena directly to the health care provider requesting the protected health information. Do not forget to include a copy of the executed HIPAA authorization and/or court order when sending the subpoena to the health care provider.

When drafting the subpoena, you must comply with the standard requirements set forth in Rule 176.1 of the Texas Rules of Civil Procedure. If you not have a validly executed HIPAA authorization or a court order, you must also provide satisfactory assurance to the covered entity that the patient has been notified that his or her protected health information has been requested.[39] This means that (1) the requesting party has made a good faith attempt to provide written notice to the individual; (2) sufficient information about the litigation in which the protected health information is requested permits the individual to raise an objection to the court; and (3) the time for the individual to raise objections has elapsed, and either no objections were filed or the objections have been resolved by the court.[40]

3. Be Mindful of the Heightened Protection Placed on Certain Records

a. Psychotherapy/Mental Health Records

Both HIPAA and the Texas medical record privacy laws have increased protections for psychotherapy and mental health records. To use an individual's psychotherapy notes – think notes (in any form) taken during the course of individual and/or family therapy sessions with a mental health professional – you must obtain the individual's authorization or the subpoena must be accompanied by a court order. Additionally, the mental health records chapter of the Texas Health and Safety Code specifically authorizes a mental health professional to disclose mental health records in a judicial proceeding affecting the parent-child relationship. Keep in mind, however, that the Texas Supreme Court has ruled that the mental health professional is not required to provide access to a child's protected mental health information if the professional

[39] 45 C.F.R. §164.512(e)

[40] *Id.*

believes that the requesting parent is not acting on behalf of the child.

b. Drug and Alcohol Treatment Records

If your case involves allegations of substance abuse, be aware that you it may be difficult to obtain medical records from any substance abuse program or facility where a party has been treated. Federal regulations under 42 U.S.C. 290dd-2 allow the release of such records under circumstances as set forth under Subsection (b)(2) of 290dd-2. 42 U.S.C. 290dd-2 (a) provides:

Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e) of this section, be confidential and be disclosed only for the purposes and the circumstances expressly authorized under subsection (b) of this section.

Subsection (b)(2) of 290dd-2 provides for three circumstances under which disclosure is permitted without the prior consent of the patient. Paragraph (C) of subsection (b)(2) provides that the content of records may be disclosed:

If authorized by an appropriate order of a court of competent jurisdiction granted after application showing good cause therefore.... In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services....

Federal regulations provide procedures for making application to a court of competent jurisdiction for the release of records that are subject to the requirements of confidentiality imposed by 42 U.S.C. 290dd-2. In particular, 42 C.F.R. 2.64 provides in relevant part that "[a]n order authorizing the disclosure of patient records for purposes other than criminal investigation or prosecution may be applied for by any person having a legally recognized interest in the disclosure which is sought." However, a fictitious name must be used to refer to any patient, and no patient identifying information can be used in the application. *Id.* Additionally, any hearing on the application must be held in the judge's chambers or in some other manner that will ensure that the identity of the patient is not disclosed to a nonparty. 42 C.F.R. ' 2.64(c). The judge may examine the contested records during the hearing. *Id.*

If you know that drug and alcohol treatment records will be needed in your case at the outset, go ahead and request the records at your temporary orders hearing or even earlier if possible.

E. Redact and/or Remove Protected Health Information from Court Filings

When filing records with the court, you should redact and/or otherwise remove any sensitive information, including protected health information, from the court filings and other documents that may become part of the public record. Be mindful of even describing the records, treatment, and/or diagnoses of a client or an opposing party in a motion or other pleading before the court. If the information is extremely sensitive, consider requesting that the records be viewed in-camera, that the courtroom be cleared before viewing the records, or that any documents referencing and discussing the sensitive protected health information be kept confidential and under seal.

Notably, the Texas Legislature recently amended the Texas Rules of Civil Procedure to further protect confidential information. Effective January 1, 2014, Rule 21c of the Texas Rules of Civil Procedure specifically precludes the inclusion of sensitive data in court filings unless the sensitive data is redacted or unless the inclusion is required by statute. Similar to the Texas Business and Commerce Code, the Rule specifically defines sensitive data as: (1) a driver's license number, passport number, social security number, tax identification number, or similar personal identification number; (2) a bank account number, credit card number or other financial account number; and (3) a birth date, a home address, and the name of any person who was a minor when the underlying suit was filed. While protected health information is not specifically listed within the Rule, it is safe to assume that the same would be precluded by virtue of the fact that certain sensitive data is in fact included within most medical and/or mental health care records.

F. Properly Dispose of Protected Health Information When the Case is Concluded

If a client file in your office contains protected health information, you must properly dispose of that information when the case is concluded. That means you must either return the protected health information to the individual or the information must be destroyed, whether in paper or electronic form. If you keep documents in paper form, it is essential that you have a shredding policy for confidential documents. This can include small electric shredders for each office as well

as contracting with HIPAA compliant shredding companies who provide shred bin containers to the office and pick up the documents on a regular basis.

VI. CONCLUSION

Although the Attorney General and OCR have yet to set their sights on family law firms, it is critical that you understand that you do qualify as a covered entity under HB 300 and are therefore subject to the federal and state laws governing the protection and confidentiality of protected health information. If you have not done so already, begin taking steps to ensure that your office is taking all necessary precautions to prevent the unauthorized disclosure of protected health information. With the increased monetary sanctions set forth in HB 300, you do not want to become the shining example of why compliance is more critical than ever before.

House Bill 300 Training Acknowledgment

On _____ I attended a 45 minute training session on the federal HIPAA Privacy and Security Rules and House Bill 300 rules regarding covered entities in Texas. The Administrative, Technical and Physical requirements of the Security rule were covered as well as the uses and disclosures of PHI in a law firm or legal department workplace.

This training was provided by Heather L. Hughes, J.D., HIPAA Privacy Officer for U.S. Legal Support, Inc. via PowerPoint presentation. Written hand-outs were included with the presentation.

Signed_____

Printed Name_____