THE RISKY BUSINESS OF HIPAA – WHY IT SHOULD MATTER TO YOU

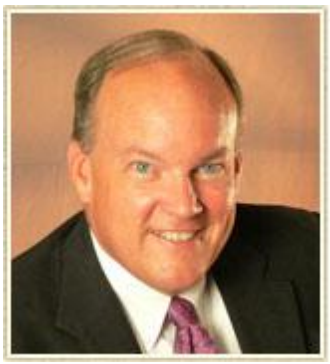
CHARLES HARDY, *San Antonio*
Higdon Hardy & Zuflacht

ANN JAMIESON, *San Antonio*
Higdon Hardy & Zuflacht

Co-Author:
SARAH DARNELL, *Denton*
KOONSFULLER, P.C.

State Bar of Texas
35th ANNUAL TEXAS FORUM:
Today's Legal Practice for Attorneys and Paralegals - Faster, Better, Stronger
March 8, 2017
Austin

CHAPTER 4



CHARLES E. HARDY
Higdon, Hardy & Zuflacht, L.L.P.
12000 Huebner Road, Suite 200
San Antonio, Texas 78230-1204
Office: 210-349-9933
Fax: 210-349-9988
E-mail: charleshardy@hhzlaw.com
Website: www.texasfamilylawinfo.com
www.hhzlaw.com

EDUCATION

B.F.A. Journalism, Southern Methodist University, Dallas, Texas (1980)
B.B.A., Business, Southern Methodist University, Dallas, Texas (1981)
J.D., St. Mary's University of San Antonio, San Antonio, Texas (1983)

PROFESSIONAL ACTIVITIES & CERTIFICATIONS

Partner - Higdon, Hardy & Zuflacht, L.L.P., San Antonio, TX
State Bar of Texas – Member, Family Law Council (2006 - present)
Texas Academy of Family Law Specialist – Past President (2012-2013), Board Member (2006-2013), Member (1989 –present)
International Academy of Matrimonial Lawyers - Member (2009-present)
American Academy of Matrimonial Lawyers - Member (2004-present), Co-Chairman of Web Committee (2012-present)
American Academy of Matrimonial Lawyers - TX Chapter: Past President (2010 – 2011), Board Member 2007 to 2011
Texas Family Law Foundation – Board Member (2013 – present)
San Antonio Family Lawyers Association – Past President (2002-2003; 1996-1997) Director (2000-2003; 1993-1997); Member (1989 to present)
Texas Monthly Magazine "Super Lawyer" – 2006 - 2016
Bexar County Domestic Relations Office Advisory Board (2002 - 2009)
Board Certified, Family Law, Texas Board of Legal Specialization (1989 – to present)
Bexar County Community Justice Program Family Law Mentor (2002 – present)
American Bar Association's Family Law Pro Bono Award 2005
San Antonio Bar Association's President's Award - 2004 & 2005
"AV Rated" by Martindale Hubbell

PUBLISHED PROFESSIONAL LEGAL ARTICLES

U. S. Enforcement of Mexican Decrees, San Antonio Family Lawyers Association, November 17, 1999, San Antonio, Texas.

Analysis of the Law and Key Issues: Procedures in Divorce Process, Texas Family Law Practice, January 27, 2000, San Antonio, TX.

Applying Procedural Tactics to Enhance Your Client's Case, Advanced Family Law Drafting Course, December 12-13, 2002, New Orleans, Louisiana.

Playing By the Rules – Using the Rules of Civil Procedure, The Rules of Evidence and the Family Code to Bolster Your Child Custody Case, San Antonio Bar Association Family Law Section Seminar, June 2003, San Antonio, TX

Advancing with the Basics – Rules of Procedure in the 21st Century, Tarrant County Family Law Bar Association, July 22, 2003, Fort Worth, TX

Extreme Billing Makeover - Successful Billing Practices and the Mutual Fairness Doctrine, San Antonio Bar Association Family Law Section Seminar, June 25, 2004, San Antonio, TX

Use of Discovery at Trial – Ultimate Trial Notebook, December 9-10, 2004, Dallas TX

New Year's Resolutions for Successful Billing Practices! (40 Rules to Making More from your Practice), San Antonio Bar Association, Family Law Section Seminar, December 21, 2004, San Antonio, TX

Discovery and Evidence: What I've Forgotten Since Law School!, San Antonio Bar Association Family Law Section Seminar, March 4, 2005, San Antonio, TX

Make More Money - Play More Golf! Increasing Billing Efficiency & Client Satisfaction!, Corpus Christi Bar Association Family Law Section, March 11, 2005, Corpus Christi, TX

Evidence and Discovery, TX Bar Advanced Family Law Course, August 8-11, 2005, Dallas, TX

Litigation Alternative – Collaborative Law, Texas

Academy of Family Law Specialists, 20th Annual Trial Institute; January 12, 2006, Reno, Nevada

Innovative ADR Litigation Options, San Antonio Bar Association, Family Law Section Seminar, March 3, 2006, San Antonio, TX

Standard of Value-How to Determine the Value of An Entity, American Academy of Matrimonial Lawyers, March 8-11, 2006, Cabo San Lucas, Mexico

Proving Attorney's Fees (Ways and Means), State Bar of Texas, Ultimate Trial Notebook Family Law 2006, December 7-8, 2006, New Orleans, Louisiana

The Mysteries of Family Law: Ten Must Know Procedures, San Antonio Bar Association, Family Law Section Seminar, March 2, 2007, San Antonio, TX

Attorneys Fees Ways and Means, The 30th Annual Marriage Dissolution Institute, May 10-11, 2007, El Paso, TX

The Mysteries of Family Law: 10 Must Know Procedure & Evidence Tips, Corpus Christi Bar Association, 2007 Family Law Seminar, October 5, 2007, Corpus Christi, TX

2008 Trial Institute, Texas Academy of Family Law Specialists, January 18-19, 2008, Santa Fe, New Mexico

Maximizing Results at Mediation, San Antonio Bar Association Family Law Section Seminar, February 29, 2008, San Antonio, TX

31st Annual Marriage Dissolution Institute, "*Electronic Evidence Panel*", State Bar of Texas, April 17-18, 2008, Galveston, TX

Co-Course Director, "*Extreme Makeover"*, San Antonio Bar Association Family Law Section Seminar, 2006, 2007, 2008

34TH Annual Advanced Family Law Course, Family Law Boot Camp, "Practice in the Trenches – Show Me the Money – Your Financial Relationship with Your Client", August 10, 2008, San Antonio, TX

34th Annual Advanced Family Law Course, "*Do I Look Like I'm Negotiating?*" Creative Mediation Techniques Panel, August 11, 2008, San Antonio, TX

Moderator, *The Divorce Lawyers and Civil District Judge Discuss Family Violence*, San Antonio Bar Association Family Law Seminar, October 30, 2008, San Antonio, TX

Co-Course Director, 2009 Trial Institute, Texas Academy of Family Law Specialists, Tampa, FL, January 16-17, 2009

Case Law Update, 2009 Parent-Child Relationships: Critical Thinking for Critical Issues, The University of Texas School of Law, January 29-30, 2009, Austin, TX

Just When You Had It Figured Out – Case Law Update, 2009 Extreme Makeover, San Antonio Bar Association Family Law Section, February 27, 2009, San Antonio, TX

Co-CLE Director, 2009 American Academy of Matrimonial Lawyers – Mid-Year Meeting, March 17-21, 2009, Kauai, Hawaii

How to Maintain Your Financial Relationship with Your Client, St. Mary's Law School, April 13, 2009, San Antonio, TX

Disproportionate Divisions, 32nd Annual Marriage Dissolution Institute, State Bar of Texas, April 16-17, 2009, Ft. Worth, TX

Your Financial Relationship with Your Client, Family Law Section, San Antonio Bar Association, April 21, 2009, San Antonio, TX

Successful Billing Practices for Family Lawyers, 31st AAML Institute, Florida Chapter of AAML, April 30-May 2, 2009, Orlando, Florida

Analyzing Your Property Case: A Prequel to Characterization, Valuation and Division of the Marital Estate, 35th Annual Advanced Family Law Course, *August 5, 2009, Dallas, TX*

Help!! My Family Lawyer Stinks!! Tips for Maintaining Good Client Relations and Protocols For Billing and Mediation Prep, 2009 Family Law Seminar, Corpus Christi Bar Association, October 2, 2009, Corpus Christi, TX

ADR Is NOT A 4-Letter Word! Hot Tops for Successful Litigation Alternatives, The University of Texas School of Law 2010 Parent-Child Relationships Seminar, Austin, Texas

Bizarre Facts & Creative Solutions, 10th Annual Family Law on the Front Lines, July 1-2, 2010, San Antonio, Texas

More Money and Less Stress: Law Office Management and Technology, State Bar of Texas 26th Annual Advanced Family Law Course, August 9-12, 2010, San Antonio, Texas

CPA's & Lawyers – A Love Affair That Can Be Taxing, San Antonio CPA Society, September 2, 2010, San Antonio, Texas

Top Technologies, Family Law Section, May 17, 2011, San Antonio, Texas

Attorney's Fees (Getting Paid for What You Do), 37th Annual Advanced Family Law Course, July 31, 2011, San Antonio, Texas

Moderator, *Technology*, 37th Annual Advanced Family Law Course, August 4, 2011, San Antonio, Texas

Top Technologies, Alamo Area Paralegals Association, September 27, 2011, San Antonio, Texas

Today's Top Thirty Tech Tips, San Antonio Bar Association, Family Law Section Seminar, February 24, 2012, San Antonio, Texas

Presenting Your Custody Case Using Technology, 38th Annual Advanced Family Law Course, August 8, 2012, Houston, Texas

2013 Texas Trial Institute, Texas Academy of Family Law Specialists, February 15, 2013, Colorado Springs, CO

Successful Billing Practices (and the Mutual Fairness Doctrine), 2013 Family Law Course 101, Advanced Family Law

Tools for Successful Mediations – Moderator, Advanced Family Law Course, August 7, 2013, San Antonio, TX

New Frontiers in Marital Property Law Course Taxes and Divorce Section – Moderator, October 3, 2013, State Bar of Texas, Napa Valley, CA

We Forgot What? Essential Protocols for Running a Successful Law Practice, Advanced Family Law Drafting 2013 Course, December 5-6, 2013, Dallas, TX

Judicial Jeopardy – Moderator, 2014 Extreme Family Law Makeover, February 28, 2014, San Antonio, TX

But He's Just a Baby! Crafting Possession & Access for Children 3 and Under – Moderator, 2014 SAFLA, June 3, 2014, San Antonio, TX

Recovering Attorney's Fees, Advanced Family Law Course Boot Camp, August 3, 2014, San Antonio, TX

Timekeeping, Billing, and Collections, Advanced Family Law Course, August 4-7, 2014, San Antonio, TX

Attorney fees in Divorce Actions, Marriage Dissolution Institute, April 9-10, 2015, Dallas, TX

Indispensable Billing Tips for All Family Lawyers: From Basics to Advanced Ideas, State Bar of Texas Annual Meeting, June 15-19, 2015, Austin, TX

Essential and Efficient Office Protocols for Every Family Law Office, Advanced Family Law Course, August 3-6, 2015, San Antonio, TX

The Application of HIPAA to Your Office and Your Clients, 39th Annual Marriage Dissolution Institute, April 7-8, 2016, Galveston, TX

Ethics of Getting Paid, State Bar of Texas Annual Meeting, June 17, 2016, Ft. Worth, TX

The Application of HIPAA to Your Office and Your Clients, Advanced Personal Injury Law Course 2016

- July 6-8, 2016, Dallas, TX
- July 27-29, 2016, San Antonio, TX
- September 14-16, 2016, Houston, TX

Anatomy of an Ethical Fee Agreement, 42nd Annual Advanced Family Law Course, August 1-4, 2016, San Antonio, TX

LANGUAGES

English, Spanish

PERSONAL

Married to Karen Maxham Hardy and the proud father of two children - my son Chase, who is attending Baylor Law School and my daughter Paige, a Sophmore at Baylor.

ANN W. JAMIESON

Higdon, Hardy & Zuflacht, L.L.P.
12000 Huebner Road, Suite 200
San Antonio, Texas 78230-1204
Office: (210) 349-9933
Fax: (210) 349-9988
Email: ajamieson@hhzlaw.com
Website: www.texasfamilylawinfo.com

EDUCATION

B.A., (Political Science), Rhodes College, Memphis, TN (2008)
J.D., St. Mary's University School of Law, San Antonio, TX (2013)

PROFESSIONAL ACTIVITIES & CERTIFICATIONS

Associate Attorney: Higdon, Hardy & Zuflacht L.L.P., San Antonio, Texas
State Bar of Texas: Member of Family Law Section
Texas Young Lawyers Association: Member
San Antonio Bar Association: Member of Family Law Section
San Antonio Young Lawyers Association: Member

PUBLISHED PROFESSIONAL LEGAL ARTICLES

The Application of HIPAA to Your Office and Your Clients, Advanced Personal Injury Law Course 2016

- July 6-8, 2016, Dallas, TX
- July 27-29, 2016, San Antonio, TX
- September 14-16, 2016, Houston, TX

The Application of HIPAA to Your Office and Your Clients, 39th Annual Marriage Dissolution Institute, April 7-8, 2016, Galveston, TX

Judicial Jeopardy, Advanced Family Law Drafting Course, December 10-11, 2015, Dallas, TX

Recovering Attorney's Fees, Advanced Family Law Course Boot Camp, August 3, 2014, San Antonio, TX

Timekeeping, Billing, and Collections, Advanced Family Law Course, August 4-7, 2014, San Antonio, TX

What About the Children: How Children of Same-Sex Couples are Left Without State-Run Support, 15 SCHOLAR 139 (2012)

PERSONAL

Born Dallas, Texas
Kappa Delta, Alumna
Phi Delta Phi (International Legal Honor's Society), Alumna

SARAH A. DARNELL

KoonsFuller, P.C.
320 West Eagle Drive, Suite 200
Denton, Texas 76201
(940) 442-6677
Fax: (940) 442-6671
sarah@koonsfuller.com

EDUCATION

- Oklahoma City University School of Law, Juris Doctor, 2006
- Sam Houston State University, Bachelor of Science in Psychology, cum laude, 2002

PROFESSIONAL ASSOCIATIONS

- Admitted to the State Bar of Texas: November 2006
- Associate Member, Annette Stewart American Inn of Court
- Member, American Bar Association (Family Law Section)
- Texas Academy of Family Law Specialists
- Denton County Bar
- Denton County Family Law Section

AWARDS AND CERTIFICATIONS

- Board Certified by the Texas Board of Legal Specialization, Family Law, *2012*
- Rising Star, Texas Super Lawyers, 2010, 2013 -2016

TABLE OF CONTENTS

HIPAA COMPLIANCE AND TRAINING FOR LAWYERS

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (more commonly referred to as "HIPAA"), is a series of federal laws aimed at protecting health information of patients by regulating the procedures of various health care providers and their business associates. Since its origination, the Act has been more than a mere nuisance to those in the health care industry for whom the act was originally intended to apply. Unfortunately for lawyers in Texas, the state legislature passed House Bill 300 in 2013 (referred to as "HB 300" in this paper), which greatly expanded the rules to apply to anyone that transmits protected health information—including lawyers. Because of HB 300, lawyers are now faced with knowing and abiding by the rules in both the Texas House Bill 300 and portions of HIPAA. The goal of this paper is to not only educate you about the federal and state laws, (including the various sanctions that can be imposed for a violation), but to also provide you with practical tools, tips to comply with the rules and a training program to take back to your office to train your staff.

II. PRE-HB 300 PRIVACY RULES

Prior to HB 300, there have always been certain protections for client privacy and confidentiality.

A. Texas Disciplinary Rules

The Texas Disciplinary Rules of Professional Conduct make it clear that lawyers shall not knowingly "reveal confidential information of a client or a former client to (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of a lawyer's law firm."[1]

"Confidential Information" includes both "privileged information" and "unprivileged client information". "Privileged Information" refers to client information that is protected under the lawyer–client privilege. "Unprivileged Client Information" is client information that is not privileged but was provided by the client and provided in the course of representation.[2]

Certainly this protected information would include a client's social security number, date of birth, address, bank account numbers, not to mention protected health information are covered by this disciplinary rule, and as such, lawyers should already be utilizing safeguards to protect this information.

B. Identity Theft Enforcement and Protection Act

Additionally, the Texas Business and Commerce Code, enacted in 2007, also applies to attorneys. Chapter 521 of the Texas Business and Commerce Code protects certain "personal identifying information" from disclosure.[3] "Personal identifying information" is defined as any "information that alone or in conjunction with other information identifies an individual, including an individual's:

A. name, social security number, date of birth or government-issued identification number;
B. mother's maiden name;
C. unique biometric data, including fingerprints, voice prints and retina or iris image.
D. unique electronic identification number, address or routing code; and
E. telecommunication access device"[4]

This provision requires businesses in general to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect [individuals] from unlawful use or disclosure of any sensitive personal information collected or maintained by the business during the regular course of business."[5]

The Act further requires the businesses destroy documents with such sensitive information by shredding, erasing, or encryption.[6]

Additionally, this Act requires that if there is a security breach that compromises such information, such breach shall be disclosed as quickly as possible to anyone whose information may be released.[7] Failure to comply with

[1] Tex. St. Rules Disc. P. 1.05.
[2] *Id.*
[3] Tex. Bus. & Com. Code §521.002.
[4] *Id.*
[5] *Id.* at §521.052.
[6] *Id.*
[7] *Id.* at §521.053.

these requirements of this section may result in a civil penalty of not less than $2,000.00 not more than $50,000.00 for each violation.[8]

A little disconcerting is that an action to enforce this provision may be brought in any county in which a violation or the county where the victim resides, or in Travis County.[9]

Finally, it is interesting to note that in addition to penalties, the Attorney General is entitled under the Act to "recover reasonable expenses including attorney's fees, court costs and investigatory costs" along with the injunctive relief for civil penalties under the Act.[10]

III. HIPAA

A. History of HIPAA

HIPAA was first issued by the Department of Health and Human Services ("HHS") on August 21, 1996 and was developed to ensure that individual's personal health information was protected by health care providers by providing regulations for storing and transferring that information.[11] The final version of the act, known as the Omnibus Rule, is the combination of previous acts throughout the course 17 years of legislation and it is located in Title 45, Subtitle A, Subchapter C of the Code of Federal Regulations in parts 160, 162 and 164.[12] Below is a simple outline of each of the subparts to HIPAA and the applicable rule next to it in bold.

Part 160- General Administrative Requirements
Subpart A- General Provisions (**Privacy Rule and Security Rule**)
Subpart B- Preemption of State Law (**Privacy Rule and Security Rule**)
Subpart C- Compliance and Investigations (**Privacy Rule, Security Rule, HITECH and Enforcement Rule**)
Subpart D- Imposition of Civil Money Penalties (**Privacy Rule, Security Rule, HITECH and Enforcement Rule**)
Subpart E- Procedures for Hearings (**Privacy Rule, Security Rule, HITECH and Enforcement Rule**)

Part 161- Reserved

Part 162- Administrative Requirements (There are more specific requirements for covered entities and business associates that are not covered in this paper because HB 300 did not include it.)
Subpart A- General provision
Subpart B-C (Reserved)
Subpart D- Standard Unique Health Identifier for Health Care Providers

Subpart E- Standard Unique Health Identifier for Health plans
Subpart F- Standard Unique Employer Identifier
Subparts G-H- (Reserved)
Subpart I- General Provisions for Transactions

Part 163- Reserved

Part 164- Security and Privacy
Subpart A- General Provisions (**Privacy Rule and Security Rule**)
Subpart B- Reserved
Subpart C- Security Standards for the Protection of Electronic Protected Health Information (**Security Rule**)
Subpart D- Notification in the Case of Breach of Unsecured Protected Health Information (**Breach Notification Rule**)
Subpart E- Privacy of Individually Identifiable Health Information (**Privacy Rule)**

[8] *Id.* at §521.151.
[9] *Id.* at §521.151(c).
[10] *Id.* at §521.151 (f)(d).
[11] *See* HIPAA for Professionals, U.S. Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/index.html (last visited on March 22, 2016).
[12] *See id.*

The first version of the Act contained what is known as the "Privacy Rule" which was published in 2000, modified in 2002, and can be found in Part 160 and 164, Subpart A and E.[13] As technology advanced and more and more covered entities were storing patient's protected health information online and through other electronic means the "Security Rule" was added which extended the Privacy Rule to electronically protected health information ("e-PHI") in 2003.[14] The Health Information Technology for Economic and Clinical Health "HITECH" Act of 2009 strengthens the Privacy Rule and the Security Rule to promote the meaningful use of technology by expanding the sanctions for violations.[15] The "Enforcement Rule" located in Subparts C, D and E of Part 160, provides the procedures for investigations through enforcement hearings and the final version of HIPAA is called the "Omnibus Rule of 2013.[16]

B. The Rules

(i) Privacy Rule: The Privacy Rule was first enacted in 2000 and is found in Part 160 Subchapters A-E as well as in Part 164 Subchapter A and E. The Rule outlines the protection of individual's health information by covered entities and business associates.

This rule applies to any "covered entity" or "business associate" as defined in 45 C.F.R. §160.103 and provides a series of regulations to protected health information (PHI).

A covered entity is one of the following: (1) Health care provider (e.g. doctors, chiropractors, nursing home, psychologist, clinics, pharmacies); (2) A Health Plan (e.g. health insurance companies, Government plans such as Medicaid or CHIPs, HMOs); or (3) A Health Care Clearinghouse.[17]

A business associate is one that assists a covered entity carry out health care functions and thus is treated like a covered entity under the rules.[18] There must be a business associate contract which details the arrangement and scope of the work done by the business associate and states that they are subject to the privacy and security rules.[19]

Disclosure means "release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.[20]

Health information means "any information, including genetic information, whether oral or recording in any form or medium that: (1) is created or received by a health care provider, health plan, public health authority, employer, lifer insurer, school or university, or health care clearinghouse; and (2) [r]elates 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."[21]

Individual means "the person who is the subject of protected health information."[22]

---

[13] *See* The HIPAA Privacy Rule, U.S. Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited on March 22, 2016).

[14] *See* HIPAA for Professionals, U.S. Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/index.html (last visited on March 22, 2016).

[15] *See id.*

[16] *See id.*

[17] 45 C.F.R. §160.103.

[18] *See id.* (stating the full definition of "business associate" as "(1) Except as otherwise provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who: (i) on behalf of such covered entity or of an organized health care arrangement (as defined in 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs or assists in the performance of: (A) A function or activity involving the sue or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting consultation, data aggregation (as defined in 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate or another covered entity."

[19] *Id.* at §164.314.

[20] *Id.* at §160.103

[21] *Id.*

[22] *Id.*

Use means "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."[23]

Violation or violate means "failure to comply with an administrative simplification provision."[24]

In general, the Secretary of the Health and Human Services cannot modify the rules more than once every 12 months.[25] The compliance date cannot be earlier than 180 days after the final modification rule is passed.[26]

If the state law is more stringent, it is valid if it provides greater protection for protected health information.[27] An entity can request that they receive an exception from the more stringent state law.[28]

Any person who believes that a covered entity or business associate is not complying with the rules may file a complaint, but the complaint must have the following: (1) must be in writing but that can be electronic form; (2) name the subject and contain a description of the act in violation; (3) filed within 180 days of the complainant knowing or having constructive knowledge but the Secretary can waive this requirement for good cause.[29] The Secretary must investigate complaint, and shall conduct a compliance review if it determines after a preliminary review of the facts that there is a possible violation due to willful neglect.[30]

A covered entity or business associate must keep records and submit compliance reports as required by the Secretary.[31] The entity must cooperate with the Secretary during the investigation and must allow the Secretary access to its facilities during reasonable periods during the investigation. The Secretary will not disclose except as necessary or enforcing compliance under the rules.[32]

If the Secretary determines that the entity is non-compliant, the Secretary shall attempt to resolve by informal means, which may include completion of corrective action plan or demonstrated compliance.[33] The Secretary must notify the covered entity or business associate and complainant (if there is one) of the actions they are taking, including any civil penalty that is being imposed.[34] A covered entity also has the option of sending written documentation of and mitigation and defenses following the breach.[35] If the Secretary is imposing civil penalty, they must inform the covered entity in the notice.[36]

In addition to disclosures, the Secretary is statutorily permitted to issue investigational subpoenas but they must contain the following: (1) name of the person; (2) statutory authority; (3) date, time and place for testimony; (4) reasonable description of the documents to produce.[37] Service is accomplished by either delivering the subpoena to a natural person or entity's principal place of business or a registered agent.[38]

The rules also make it clear that the covered entity or business associate shall not intimidate or retaliate against any individual that files a complaint or testifies in a hearing or other procedure.[39]

There are specific ways in which protected health information can be released, the first of which is through a valid authorization.[40] The general rule governing authorization is that a covered entity must obtain a valid authorization prior to disclosing any protected health information.[41] There are even specific rules governing the disclosures of psychotherapy notes, and disclosures for marketing or sales. [42]

---

[23] *Id.*
[24] *Id.*
[25] *Id.* at §160.104.
[26] *Id.*
[27] *Id.* at §160.203.
[28] *Id.* at §§160.204-160.205.
[29] *Id.* at §160.306.
[30] *Id.* at §160.308.
[31] *Id.* at §160.310.
[32] *Id.*
[33] *Id.* at §160.312.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.* at §160.314.
[38] *Id.*
[39] *Id.* at 160.316.
[40] *Id.* at §164.502.
[41] *Id.* at §165.508 (stating "(a) *Standard: Authorizations for uses and disclosures*—(1) *Authorization required: General rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.").
[42] *See id.* ("(2) *Authorization required: Psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes,

The general standard is that a covered entity and business associate may not disclose protected health information except as provided in Subpart C of Part 160.[43] For a covered entity, the *permitted* uses and disclosures include disclosing (1) to the individual; (2) for the treatment or payment of a treatment; (3) incident to a use or disclosure.[44] A covered entitled is *required* to disclose to an individual under 45 C.F.R §164.524 or 45 C.F.R. §164.528 and when the Secretary of the Health and Human Services is doing a compliance investigation.[45] A business associate is permitted to use protected health information by its contract or other arrangement and it is required to disclose when required by the Secretary and to covered entities under §164.524(c)(c)(ii) and (3)(ii).[46]

Additionally, the rule outlines the organizational requirements for regular protected health information. Business associate contracts must establish permitted uses and disclosures of protected health information and how safeguards, reporting breaches, internal practices, termination procedures will be governed.[47]

An authorization must contain these core elements: (1) a description of the information to be used or disclosed; (2) the name of persons or class of persons; (3) names of those authorized to disclose information to: (4) description of the purpose or use of the disclosure; (5) the expiration date; (6) the signature of individual that also must contain a date; and the required statements that the individual has a right to revoke the authorization and how that can be done.[48] Finally, the authorization must be written in plain language and a copy of the executed authorization must be provided to the individual.[49]

As stated above an authorization is required generally required and the disclosure must be within the scope of the authorization.[50] There is however, an exception for psychotherapy notes.[51] The course of the person's treatment is protected from disclosure. Additionally, a covered entity may disclose protected health information without an authorization when a covered entity is using the protected health information to defend itself against an allegation.[52] An authorization can also obviously not be defective.[53] Such a defect includes there not being any expiration date, an incomplete authorization, a revoked authorization or one that contains false information.[54]

Additionally the covered entity may use or disclose PHI and give the opportunity for the individual to agree or object except in the case of emergency circumstances, which are bypassed if they are consistent with prior expressed belief and the individual's best interest, if the individual is deceased or in the case of a natural disaster.[55] However, this notice is not required if the entity is preventing or controlling disease, child abuse or neglect, in the event of an FDA investigation, to a school (where the individual is a student and it is their immunization record), to the parent of an un-emancipated child.[56] It is important to note that this section states that a covered entity can disclose to a government agency if there is abuse or neglect, but the entity must inform the individual that they are doing so.[57] The only exception to this rule is if the notification would place that individual at risk.[58]

There are also certain exceptions and rules for the health information of veterans, individuals in the custody of law enforcement, and those with information on the instant national criminal background check system.[59]

An individual has a right to have notice of how their protected health information will be used including a header, description with at least one example, a description of other purposes, that individual's rights, the covered

---

except:(i) To carry out the following treatment, payment, or health care operations: (A) Use by the originator of the psychotherapy notes for treatment; (B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or (C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and (ii) A use or disclosure that is required by §164.502(a)(2)(ii) or permitted by §164.512(a); §164.512(d) with respect to the oversight of the originator of the psychotherapy notes; §164.512(g)(1); or §164.512(j)(1)(i).").

[43] *See id.* at §164.502.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *See id.* at §164.504.
[48] *Id.* at §164.506.
[49] *Id.*
[50] *Id.*
[51] *See id.* at §164.508.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.* at §164.510.
[56] *Id.* at §164.512.
[57] *Id.*
[58] *Id.*
[59] *Id.* at §164.514.

entities' duties, description of how complaints will be handled including a contact number.[60] The notice must contain an effective date and the entity must notify the individual of any revisions in writing every three years.[61]

A covered entity must also permit an individual from restricting access to certain information, but a covered entity is not required to agree to a restriction except in the case of where the disclosure is for a purpose of payment and is not required by law or the payment was received in full.[62] An individual has a right of access to their protected health information except for: psychotherapy notes, information gathered in anticipation of civil, criminal or administrative action.[63] Note that there are very specific guidelines for this including that it must be in readable form and, if the entity is denying the request, they must provide them with a description and it can be a summary if the individual agrees to receive the summary form.[64] They must provide the information in a reasonable time.[65] If the individual requires a summary of the fees, the covered entity must provide a summary of the cost-based fee including labor, supplies, fees and postage.[66] If there is a denial, the entity must provide the basis for the denial and statement of individual's right to review, the complaint procedures.[67] If it is another's responsibility to maintain the records, they must provide them with their contact information.[68]

A separate person must review any denial of a request for information.[69] The office must have record sets that an individual has a right to obtain as well as the names of persons and titles of persons overseeing the record sets and requests of individual.[70]

An individual has a right to request their record be amended.[71] The entity in turn has a right to deny them of that if they are not the originator of the record, not part of the requested record set, or would not otherwise be available for inspection.[72] If accepting amendment, the entity must make the amendment and inform the individual that amendment was made and request their acceptance to send update to necessary persons.[73] If denying the request, the denial must be in plain language and state the basis for the denial, the individual's right to file a statement of disagreement and complain.[74] The entity can then file a rebuttal statement and must provide that to the individual as well as keep a record of it.[75] It is required that the entity respond to the request within 60 days from when the request was made but this can be extended in specific situations outlined in §164.526.[76] The entity must keep documents related to the amendment.[77] A covered entity that is informed of an amendment by another covered entity must amend their record.[78]

An individual has a right to an accounting of disclosures the entity made for the prior six years; however there are numerous exceptions and regulations for this.[79]

A privacy official must be appointment by each covered entity that will be responsible for implementation of procedures for that covered entity.[80] It is also required that a covered entity have a contact person for complaints.[81] Finally, there is a requirement by the federal rules that each covered entity train its employees of the rules in relation to their position.[82] The time for this training to occur was the compliance date that applied to the type of covered entity or business associate and any new employee must receive the training within a reasonable amount of time and if there is a material change to the rules, the employees must receive the training within a reasonable amount of time

---

[60] *Id.* at §164.520.
[61] *Id.*
[62] *Id.* at §164.522.
[63] *Id.* at 164.524.
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.* at 164.526.
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.* at §164.528.
[80] *Id.* at §164.530.
[81] *Id.*
[82] *Id.*

after the change becomes effective.[83] The statute also requires that the training be documented by the entity.[84] The entity is required to safeguard PHI from unintentional or incidental uses or disclosures or disclosures that are in violation of the rule.[85] The covered entity must also have a complain procedure in place.[86] The covered entity must keep documentation of all of the complaints received which includes disposal of the complaints.[87] Sanctions for employees who violate the company's policies and procedures must be implemented.[88] The covered entity also has a duty to mitigate harmful effects from violating.[89]

The covered entity is required to refrain from intimidating or retaliating against the individual to waive his/her rights including filing a complaint.[90] The entity also cannot require an individual to sign a waiver of rights under this section as a condition of their treatment.[91] A covered entity must develop its own policies and procedures to ensure its compliance and must make changes if law changes and must be documented.[92] If the change to a policy or procedure does not affect the notice, then it doesn't need to be changed. The documentation can be in writing or in electronic form.[93] The retention period is the later of six years from the creation date or when it was last in effect.[94]

(ii) Security Rule: Enacted in 2003, the Security Rule sought to expand the applicability of the privacy rules to electronic protected health information ("e-PHI").[95] The Security Rule is located in Part 160 and Part 164, Subparts A and C. The focus is of the rule is how to safeguard protected health information in the new technology age.[96] The rule applies to all covered entities and their business associates.[97] The general rules require the covered entity to protect against anticipated threats, but the rule allows the consideration of several factors for a covered entity to consider when developing their security plan.[98] Those factors include: (1) the size of the covered entity and the number of patient's protected health information being stored; (2) the infrastructure of the entity; (3) the cost of the security measures and (4) the probability of risk.[99] Certain administrative requirements include: risk analysis; risk management; sanction policy for employees who fail to comply with the entities' plan; information system account review, assigned security procedures for authorization and supervision, implementation security awareness and training program; and the log-in monitoring, and password management.[100]

Required physical safeguards include: (1) disaster recovery plan (such as a fire in the electrical room where your server is stored); (2) media re-use; (3) disposal plan; (4) accountability and maintenance records of hardware and electronic media; (5) data back-up and storage.[101] The technical safeguards (or access control), requires that (1) each employee has unique user identifications and are assigned a unique name and number; (2) emergency access procedure; (3) automatic logoff of a computer; (4) encryption and decryption; person/entity authentication and transmission security.[102]

Additionally, the security rule requires certain organizational requirements including that each entity obtains a business association model contract which provides that the business associate shall comply with the requirements outlined in the Security Rule and that the business associate shall report any breach to the covered entity.[103]

A covered entity or business associate is allowed to change their policies and procedures, but they must keep documentation of the changes and they must be in electronic form.[104] If a document is required by their policies, they

---

[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *See* The Security Rule, U.S. Department of Health & Human Services, http://www.hhs.gov/hipaa/for-professionals/security/index.html (last visited on March 22, 2016).
[96] *See Id.*
[97] *See id.*; *see also* 45 C.F.R. §164.302.
[98] *Id.* at §164.306.
[99] *Id.*
[100] *Id.* at §164.308.
[101] *Id.* at §164.310.
[102] *Id.*
[103] *Id.* at §164.314.
[104] *Id.* at §164.216.

must also maintain that documentation.[105] The implementation requirements are that the policy and procedure must provide a time limit (6 years) and availability and provide periodic updates.[106]

The compliance dates for initial implementation varied slightly between different entities, but in no event was the compliance year later than 2006.[107]

Below is the security standards matrix contained in Appendix A to Subpart C of Part 164, which outlines the requirements and suggestions for safeguarding electronically stored protected health information.[108]

Standards	**Sections**	**Implementation Specifications (R) = Required, (A) = Addressable**
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)

[105] *Id.*
[106] *Id.*
[107] *Id.* at §164.318.
[108] *Id.* at Appendix A to Subpart C of Part 164—Security Standards: Matrix.

		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards (see §164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

(iii) HITECH and Enforcement Rule:

HITECH was enacted in 2009 and provided the procedural mechanisms for enforcement of the Rules which ultimately strengthened the rules.[109] The rules are contained in Part 160, Subparts C, D and E, which were more particularly described with the Privacy Rule and Security Rules above.

(iv) Breach Notification Rule: The Breach Notification Rule answers the question of what a covered entity or business associate should do in the event that their security mechanisms for ensuring the safety of protected health information are compromised. The rule is contained in Part 164, Subpart D of the Code of Federal Regulations and applies to breaches on or after September 23, 2009.[110] "Breach" is defined as "acquisition, access, use, or disclosure of protected health information not permitted which compromises the privacy or security of protected health information."[111] The definition does not include (1) the unintentional access to PHI by a worker who is acting in good faith and does not further the disclosure; (2) the inadvertent disclosure of a person who is authorized to access and not further disclosed to anyone else; (3) disclosure by a covered entity or business associate and the unauthorized person could not reasonably have returned.[112] There is also a risk assessment that is concerned in determining the extent of the breach.[113] That assessment includes considering: (1) the nature and extent of the protected health information involved (including types of identifiers); (2) unauthorized person who used the protected health

[109] *SEE* HITECH ACT ENFORCEMENT INTERIM FINAL RULE, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, HTTP://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SPECIAL-TOPICS/HITECH-ACT-ENFORCEMENT-INTERIM-FINAL-RULE/INDEX.HTML (LAST VISITED ON MARCH 22, 2016).

[110] *SEE* BREACH NOTIFICATION RULE, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, HTTP://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/BREACH-NOTIFICATION/INDEX.HTML (LAST VISITED ON MARCH 22, 2016); *SEE ALSO* 45 C.F.R. §164.400.

[111] 45 C.F.R. §164.402.

[112] *Id.*

[113] *Id.*

information; (3) whether protected health information was actually acquired or viewed and (4) the extent the risk can be mitigated.[114]

Once the breach has occurred, there are certain notification requirements that the entity must comply with. The first type of notification required is the notification to the individuals affects.[115] The entity is required to notify all individuals affected by the breach within sixty (60) days.[116] (The timeline starts from the first day the entity became aware of the breach or through due diligence should have known about the breach.)[117] The notification must be written and include a brief description of the breach including dates, type of PHI involved, steps the individual should take to protect oneself, investigation the covered entity is undergoing, and contact procedures for more information.[118]

In addition to notifying the individual, the entity must notify the media if the breach involved more than 500 individuals in the state.[119] The entity must also notify the Secretary of the U.S. Department of Health and Human Services if the breach of unsecured PHI involved more than 500 individuals.[120] If the beach involved less than 500 individuals, the entity is required to maintain a log of the individuals affected.[121] If a business associate causes the breach, they have a duty to notify the covered entity and have similar requirements as the covered entities.[122] Finally, the burden of proof is on the covered entity to show they complied with the breach notification rule.[123]

(v) The Final Omnibus Rule: The Final Omnibus Rule contains the final versions of the Privacy Rule, Security Rule, HITECH and the Enforcement Rule and the Breach Notification Rule.[124] The Omnibus Rule became effective in 2013 and continues as the most recent version of HIPAA rules, which has been included in the analysis of the other rules.

It is important to note that the rules make it clear that HIPAA only applies to covered entities and business associates and after a review of these definitions, it is clear that lawyers are not covered by HIPAA, which leads to our next topic of HB 300.

IV. TEXAS HOUSE BILL 300/ TEXAS HEALTH & SAFETY CODE CHAPTER 181

This statute is more commonly referred to as "HB 300" (which was subsequently codified in Chapter 181 of the Texas Health and Safety Code). HB 300 adopted many aspects of HIPAA, but it also expanded and modified certain aspects of HIPAA. Most notably, HB 300 greatly expanded the definition of "covered entity" to now include anyone who engages in the practice of obtaining or transferring protected health information.[125] The statute does not affect any statute that provides greater protection of protected health information.[126] This chapter controls where there is a conflict with another chapter, except §58.0052 of the Family Code (the juvenile justice inter-agency sharing of non-educational records).[127] Section 181.004 states that entities must comply with the state and federal laws.[128] In Texas, the executive commissioner is charged with administering this subchapter (compared with the Secretary of the Health and Human Services for the federal laws), which includes reviewing 45 C.F.R. Parts 160 and 164 that are amended after September 2011 and if the executive commissioner determines they are appropriate, it shall adopt those rules as state law.[129] In determining whether to adopt a rule, the executive commissioner shall consider the following: the adverse and beneficial effects the amendment has on the lives of the individual and their expectations of privacy and the government entities, institutions and hospitals and businesses in the state.[130] The executive commissioner shall report their determination and file it with the presiding officer of each house and before the thirtieth day after the

---

[114] *Id.*
[115] *Id.* at §164.404.
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.* at §164.406.
[120] *Id.* at §164.408.
[121] *Id.*
[122] *Id.* at §164.410.
[123] *Id.* at §164.414.
[124] *SEE* OMNIBUS HIPAA RULEMAKING, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, HTTP://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/PRIVACY/LAWS-REGULATIONS/COMBINED-REGULATION-TEXT/OMNIBUS-HIPAA-RULEMAKING/INDEX.HTML (LAST VISITED ON MARCH 22, 2016).
[125] *See* Tex. Health & Safety Code §181.001.
[126] *Id.* at §181.002.
[127] *Id.*
[128] *Id.* at §181.004.
[129] *Id.* at 181.005.
[130] *Id.*

report which explains the reasons behind the executive commissioner's determination.[131] The Texas statute makes it clear that protected health information under the statute is not information that is publically disclosed.[132]

There are several exemptions for certain types of organizations. A partial exemption exists for a covered entity that is under §602.001 of the Insurance Code and an entity that is established under Article 5.76-3 of the Insurance Code or an employer.[133] Section 181.052 also provides a covered entity a right to process payment transactions by acting as a financial institution to process payments without having to comply with the act.[134] So long as a nonprofit agency's purpose is not primarily to provide health care, the nonprofit is exempt from the executive commissioner to the extent that the agency pays for prescriptions or health care for an individual.[135] Additionally, the chapter does not apply to worker's compensation insurance or someone working in connection to it, or to an employee benefit plan or an entity's own employee.[136] The American Red Cross is also permitted special authorization to them to access information that is needed to address emergency relief.[137] Also, the chapter does not apply to an agency that is treating an individual with a mental impairment, educational records and crime victim compensation.[138]

The Texas definition states: "(2) "Covered entity" means any person who: (A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site; (B) comes into possession of protected health information; (C) obtains or stores protected health information under this chapter; or (D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information."[139]

Compare this lengthy definition which basically includes anyone who comes into possession of protected health information (including family lawyers), with the original definition of covered entity outlined in HIPAA: "Covered entity means (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."[140] It is apparent that the Texas legislature greatly expanded the definition to include numerous entities outside of the health care industry.

Since other entities, including lawyers are now required to follow the state statutes, it is important to understand those requirements in detail. Each covered entity shall provide training for its employees regarding the state and federal law on protected health information as is appropriate for that employee's specific duties.[141] The training must

---

[131] *Id.*
[132] *Id.* at §181.006.
[133] *Id.* at §181.051.
[134] *Id.* at §181.052.
[135] *Id.* at §181.053.
[136] *Id.* at §181.054.
[137] *Id.* at §181.056.
[138] *See id.* at §§181.057, 181.058, 181.059.
[139] *See id.* at §181.001 "(2-a) "Disclose" means to release, transfer, provide access to, or otherwise divulge information outside the entity holding the information. (2-b) Repealed by Acts 2015, 84th Leg., ch. 1 (S.B. 219), § 3.1639(55). (3) "Health Insurance Portability and Accountability Act and Privacy Standards" means the privacy requirements in existence on September 1, 2011, of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) contained in 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E. (4) "Marketing" means: (A) making a communication about a product or service that encourages a recipient of the communication to purchase or use the product or service, unless the communication is made: (i) to describe a health-related product or service or the payment for a health-related product or service that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: (a) the entities participating in a health care provider network or health plan network; (b) replacement of, or enhancement to, a health plan; or (c) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (ii) for treatment of the individual; (iii) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; or (iv) by a covered entity to an individual that encourages a change to a prescription drug included in the covered entity's drug formulary or preferred drug list; (B) an arrangement between a covered entity and any other entity under which the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service; and (C) notwithstanding Paragraphs (A)(ii) and (iii), a product-specific written communication to a consumer that encourages a change in products. (5) "Product" means a prescription drug or prescription medical device.").
[140] 45 C.F.R. §160.103.
[141] Tex. Health & Safety Code §181.101.

occur within 90 days after the employee is hired by the entity and if a material change occurs to either the federal or state law, the employer must train the employees within a reasonable time period, but in no event can that time period be less than one year after the law is effective.[142] The employee must sign in writing or electronically that verifies the employee's completion of the required training. [143]

In addition to understanding who is covered under each of the federal and state rules, it is important to understand as a "covered entity" under HB 300 that there are also very specific guidelines which govern the disclosure of PHI to order to avoid any violations. Each individual is entitled to their personal record in electronic form within 15 days after the receipt of the request and cannot require the entity to provide any part of the protected health information that is exempt under federal law 45 C.F.R. §164.524.[144]

As part of the responsibilities of the attorney general, a consumer information website is required to be maintained.[145] The website includes information for individuals about their privacy rights under both federal and state law, a list of agencies that regulate various covered entities and information about the agency's complaint process as well as their contact information.[146] The website can be accessed at the following URL: https://texasattorneygeneral
.gov/cpd/state-\andfederal-health-privacy-laws. It is interesting to note that the State Bar of Texas is not listed as one of the organizations receiving complaints. The authors suspect that this absence is merely a result of the state's focus on the medical field. While the focus for now seems to be on those entities in the health care industry, it is clear that the attorney general could turn its attention to attorneys at any point in time. Another requirement under HB 300, is that the attorney general file an annual report to the legislature with the type of complaints and numbers received by the attorney general and state agencies and the enforcement action that was taken in response to the violations.[147] Additionally, each agency shall submit information about the complaints they received but the attorney general shall de-identify the protected health information in the report.[148] A person or entity cannot re-identify a person's identity without first obtaining that person's consent.[149]

Upon review of the 2015 report filed by the attorney general, 717 complaints total, including 38 consumer complaints received directly by the attorney general, and out of the 717 complaints, 588 of those were regarding the unlawful disclosure of protected health information.[150] Among remedies reported by the attorney general were fines, counseling, retraining, remedial plans and reprimands. Several lawsuits were also filed.

The statute goes on to discuss the marketing uses for protected health information. In order to use an individual's protected health information for marketing, the entity must obtain an unambiguous consent to disclose an individual's protected health information, but there are exceptions if the individual requested the marketing, if the communication is face-to-face, if it is related to a needed patient assistance program or a "promotional gift of nominal value provided by the covered entity".[151] If a covered entity sends a mailer, it must only contain a name and address and must contrail the name and toll-free telephone number for the entity that sent it.[152] A covered entity cannot sale an individual's protected health information, except to another covered entity within the course of treatment, payment or other operation, or as authorized by state or federal law.[153] In general, if a covered entity is receiving protected health information and it is subject to electronic disclosure, the entity must notify the individual in a formal notice as outlined by the statute.[154] This is a similar requirement as the federal privacy and security rules. There are, of course, exceptions to the rule.[155]

---

[142] *Id.*
[143] *Id.*
[144] *Id.* at §181.102.
[145] *Id.* at §181.103.
[146] *Id.*
[147] *Id.* at §181.104.
[148] *Id.*
[149] *Id.* at §181.151.
[150] *See* Texas Medical Records Privacy Act Annual Report: Fiscal Year 2015, Office of the Attorney General.
[151] Tex. Health & Safety Code §181.152.
[152] *Id.*
[153] *Id.* at §181.153.
[154] *Id.* at §181.154.
[155] *See Id.* ("(c) The authorization for electronic disclosure of protected health information described by Subsection (b) is not required if the disclosure is made: (1) to another covered entity, as that term is defined by Section 181.001, or to a covered entity, as that term is defined by Section 602.001, Insurance Code, for the purpose of: (A) treatment; (B) payment; (C) health care operations; or (D) performing an insurance or health maintenance organization function described by Section 602.053, Insurance Code; or (2) as otherwise authorized or required by state or federal law. (d) The attorney general shall adopt a standard authorization form for use in complying with this section. The form must comply with the Health Insurance Portability

V. WHY SHOULD I CARE?

A. HIPAA Violations and Injunctive Relief:

There are serious repercussions that an attorney may face if they are not HIPAA compliant. The penalty for a breach of protected health information depends on the severity of the breach and whether the breach was due to negligence or was intentional. The Department of Health and Human Services, Office of Civil Rights (OCR) is in charge of administrating and enforcing the standards set forth by the rules. They have the ability to conduct compliance reviews and assess civil and criminal penalties for noncompliance.

1. Civil:

The first type of penalty one could face for noncompliance is a civil monetary penalty. This type of penalty is assessed even if there was mere negligence on the part of the covered entity. Each level of sanction assessed depends on the type of fault involved. "Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."[156] The general rule for the basis for a civil monetary penalty is that the Secretary shall impose a civil monetary penalty on a covered entity or business associate if it is found responsible for a violation.[157] For violations that involve more than one covered entity or business associate, the Secretary can impose a sanction on each covered entity member of an affiliated covered entity and hold them jointly and severally liable unless another member of the affiliated covered entity is found to be responsible for the violation.[158] The Secretary can also impose a sanction on the covered entity or business associate under common law agency.[159] Infractions that occurred before February 18, 2009, the Secretary cannot impose a civil penalty more than $100 for each violation or in excess of $25,000 for identical violations during a single calendar year.[160] However, the penalties assessed after February 18, 2009 are much more severe. If the Secretary establishes that a covered entity or business associate did not have knowledge and would not have even through the exercise of due diligence, it cannot impose a sanction less than $100 but not more than $50,000 for each violation or in excess of 1.5 million dollars in a single calendar year.[161] If the violation was not due to willful negligence, the Secretary cannot impose a sanction less than $1,000, but not more than $50,000 or in excess of 1.5 million dollars in a single calendar year.[162] If the violation is due to willful neglect, but is corrected within 30 days, the amount cannot be less than $10,000 or greater than $50,000 or in excess of 1.5 million dollars.[163] Finally, if the violation is due to willful neglect it is not corrected within 30 days, the penalty imposed cannot be less than $50,000 for each violation or in excess of 1.5 million dollars for identical violations in one year.[164] Additionally, the Secretary will determine the number of violations and in the case where an entity has a continuing violation the Secretary is permitted to assess the violations as if each violation is a separate violation each day.[165]

There are various factors that the OCR will evaluate prior to assessing a civil penalty and they are outlined in §160.408. These factors include:

> (a) [t]he nature and extent of the violation, consideration of which may include but is not limited to: (1) [t]he number of individuals affected; and (2) [t]he time period during which the violation occurred; (b) [t]he nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to: (1) [w]hether the violation caused physical harm; (2) [w]hether the violation cause financial harm; (3) [w]hether the violation resulted in harm to an individual's reputation; and (4) [w]hether the violation hindered an individual's ability to obtain health care; (c) [t]he history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, or business associate, consideration of which may include but is not limited to: (1) [w]hether the current violation is the same or similar to previous indications of noncompliance; (2) [w]hether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance; (3) [h]ow the covered entity or business associate has responded to technical assistance from the Secretary provided in the context

---

and Accountability Act and Privacy Standards and this chapter. (e) This section does not apply to a covered entity, as defined by Section 602.001, Insurance Code, if that entity is not a covered entity as defined by 45 C.F.R. Section 160.103.").

[156] 45 C.F.R. §160.401.
[157] *Id.* at §160.402.
[158] *Id.*
[159] *Id.*
[160] *Id.* at §160.404.
[161] *Id.*
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Id.* at §160.406.

> of a compliance effort; and (4) [h]ow the covered entity or business associate has responded to prior complaints; (d) [t]he financial condition of the covered entity or business associate, consideration of which may include but is not limited to: (1) [w]hether the covered entity or business associate had financial difficulties that affected its ability to comply; (2) [w]hether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and (3) [t]he size of the covered entity or business associate; and (e) [s]uch other matters as justice may require.[166]

There are affirmative defenses outlined in §160.410. For violations on or after February 18, 2009, the Secretary may not impose a civil penalty on a covered entity or business associate if it establishes the violation was not due to willful neglect and it corrected either during the 30 days from when it knew or would have known through the exercise of due diligence or such additional periods prescribed by the Secretary.[167] But note that the Secretary can waive a civil penalty that would be excessive in light of the violation.[168] Violations must be brought forth within 6 years from the date of occurrence otherwise it is barred by the statute of limitations.[169] The Secretary is also provided with authority to settle cases.[170] A penalty found under subchapter D does not limit a penalty under another area of law.[171]

If the Secretary is imposing a penalty, they must send a notice containing: (1) the penalty's statutory basis; (2) description of the findings and reasons the violations on the part of the Respondent subject them to a penalty; (3) amount and its reference to §160.404; (4) any circumstances that apply from §160.408; (5) instructions for a response to the notice.[172] The Respondent can request a hearing before an administrative law judge.[173] If, however, the Respondent fails to request a hearing within 90 days, the Secretary shall impose the penalty and inform the Respondent the procedure for satisfying the penalty.[174] The collection of the penalty may be sought through a civil action, but no defense that is not raised in a hearing before an administrative law judge may be brought up in a civil action.[175] Additionally, the Secretary may notify the state where the entity is located and any organization or licensing authority of the entity's violation.[176] The detailed procedure for the hearing before the administrative law judge is governed by Subpart E.

2. Criminal:

A criminal sanction may be assessed in a more egregious violation such as the intentional selling of protected health information. The Department of Justice is charged with carrying out the prosecution for such violations and they can include up to ten years of imprisonment.

B. Texas House Bill 300:

Any violation of Chapter 181 of the Texas Health and Safety Code is administered by the Office of the Attorney General and similar to the HIPAA enforcement provisions, the severity of the penalty depends on the extent and motivation behind the breach. The first form of enforcement that is used is injunction relief.[177] The second form of enforcement is through fines which vary depending on the *mens rea* behind the breach and whether there was any attempt to mitigate the damage. The penalties include: 1) $5,000 for each violation in one year if the violation was committed negligently; 2) $25,000 if the violation was committed knowingly or intentionally; and 3) $250,000 if the covered entity knowingly or intentionally committed the breach for profit.[178] The state also provides other disciplinary action which can include probation by the entity's licensing agency.[179]

---

[166] *Id.* at §160.408.
[167] *Id.* at §160.410.
[168] *Id.* at §160.412.
[169] *Id.* at §160.414.
[170] *Id.* at §160.416.
[171] *Id.* at §160.418.
[172] *Id.* at §160.420.
[173] *Id.*
[174] *Id.* at §160.422.
[175] *Id.* at §160.424.
[176] *Id.* at §160.426.
[177] *See* Tex. Health & Safety Code §181.201 (stating "(a) The attorney general may institute an action for injunctive relief to restrain a violation of this chapter.").
[178] *See id.* (providing that "(b) In addition to the injunctive relief provided by Subsection (a), the attorney general may institute an action for civil penalties against a covered entity for a violation of this chapter. A civil penalty assessed under this section may not exceed: (1) $5,000 for each violation that occurs in one year, regardless of how long the violation continues during that

VI. WI-FI AND EMAIL SECURITY

One of the most vulnerable places that we store and access PHI is through the internet, and more specifically, through our emails. Today's hackers have many tools at their disposal and their gain in accessing PHI is potentially our HIPAA violation.

A. Wi-Fi

It has become relatively easy for hackers to access unsecure Wi-Fi networks or set up fake public Wi-Fi networks in coffee shops and airports to access computers from nearby customers looking to use "free Wi-Fi." Additionally, there are downloadable tools and even cheap hardware. (For one hundred dollars, someone can buy a "Pineapple" device that allows them easy access to your emails, messages and browser sessions).

Encryption is absolutely essential to protecting PHI from potential hackers. Encryption acts a "scrambler" of the information so it is more difficult to initially break into and, in the event it is obtained, the unauthorized user will not be able to read or interpret the content since they do not have the encryption key.

There are two main types of wireless security encryption in the technology universe. The first is Wired Equivalent Privacy (WEP) and the second is Wi-Fi Protected Access (WPA). Most techies advise against using WEP because it is no longer considered to be very secure and hackers today have many tools available to crack any WEP password within a few minutes. WPA or WPA2 (which is the current standard) is more secure because it uses a longer key. WPA and WPA2 provide two mode options: personal and enterprise. Personal is likely the mode you use for your personal computer at home and it contains a pre-shared key (i.e. a password that you set up on your router and your computer). It is recommended that you use a strong password of at least 13 mixed characters and no common words for your personal WPA connection. An Enterprise mode is used by most businesses. It is also known as "RADIUS," which stands for "Remote Authentication Dial in User Server," and uses a separate RADIUS server or host that provides greater security.

B. Email

Another way that hackers can access PHI is through your email; therefore, encryption of your email is also essential to protect you from an unauthorized disclosure of PHI. There are three main components of email that should be encrypted: email connections, the emails themselves, and stored or archived emails.

---

year, committed negligently; (2) $25,000 for each violation that occurs in one year, regardless of how long the violation continues during that year, committed knowingly or intentionally; or (3) $250,000 for each violation in which the covered entity knowingly or intentionally used protected health information for financial gain. (b-1) The total amount of a penalty assessed against a covered entity under Subsection (b) in relation to a violation or violations of Section 181.154 may not exceed $250,000 annually if the court finds that the disclosure was made only to another covered entity and only for a purpose described by Section 181.154(c) and the court finds that: (1) the protected health information disclosed was encrypted or transmitted using encryption technology designed to protect against improper disclosure; (2) the recipient of the protected health information did not use or release the protected health information; or (3) at the time of the disclosure of the protected health information, the covered entity had developed, implemented, and maintained security policies, including the education and training of employees responsible for the security of protected health information. (c) If the court in which an action under Subsection (b) is pending finds that the violations have occurred with a frequency as to constitute a pattern or practice, the court may assess a civil penalty not to exceed $1.5 million annually. (d) In determining the amount of a penalty imposed under Subsection (b), the court shall consider: (1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure; (2) the covered entity's compliance history; (3) whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose protected health information is involved in the violation; (4) whether the covered entity was certified at the time of the violation as described by Section 182.108; (5) the amount necessary to deter a future violation; and (6) the covered entity's efforts to correct the violation. (e) The attorney general may institute an action against a covered entity that is licensed by a licensing agency of this state for a civil penalty under this section only if the licensing agency refers the violation to the attorney general under Section 181.202(2). (f) The office of the attorney general may retain a reasonable portion of a civil penalty recovered under this section, not to exceed amounts specified in the General Appropriations Act, for the enforcement of this subchapter.").

[179] *See id.* at §181.202, ("In addition to the penalties prescribed by this chapter, a violation of this chapter by a covered entity that is licensed by an agency of this state is subject to investigation and disciplinary proceedings, including probation or suspension by the licensing agency. If there is evidence that the violations of this chapter are egregious and constitute a pattern or practice, the agency may: (1) revoke the covered entity's license; or (2) refer the covered entity's case to the attorney general for the institution of an action for civil penalties under Section 181.201(b).").

Email connections can be encrypted through the use of a Secure Socket Layer (SSL) and Transport Layer Security (TLS). It is important to make sure that one of these security measures is activated on the particular device wherein you will be accessing your email. You can easily tell if one of those measures is enacted by looking at the URL. If SSL is enacted, the URL should begin with "https" instead of "http." If you use Microsoft Outlook, you will have to review the options menu to see whether the email connection is encrypted since there is no visible URL.

The second component that needs to be encrypted is the email itself. This component is more cumbersome since it requires action on the part of the sender of the email and the recipient. Depending on your particular email service provider, you might already have encryption services that you do not know about. If not, you can download the encryption software or add-on that is needed to encrypt your emails. Secure/Multipurpose Internet Mail Extensions or "S/MIME" requires that you download a certificate on your computer and provide the email recipient with the public key prior to sending the encrypted email. Then, once the recipient receives the encrypted email, they will simply type in the previously provided public key and be able to read the encrypted email. S/MIME is available through many email service providers including Microsoft Outlook, and is available as an add-on to other email service providers like Gmail and Hotmail. Important Note! A standard Gmail, Hotmail, Yahoo, or other email address is easily accessed and is much more vulnerable to a hacker.

Finally, it is important that the emails that you are storing or archiving are also protected. The first way to do this is by fully encrypting your mobile devices and laptop by having a required login to access the device. This encryption is offered automatically on the iPhone and Mac products and is now available on most Android devices. In addition to full encryption of the device itself, consider also encrypting the folders where your stored emails are contained. For Microsoft Windows users, you can utilize the Encrypted File System (EFS) feature that comes with most versions of the software. You will need to find where your archived emails are being stored on your computer and encrypt that folder by merely accessing the folder's properties and selecting the encryption option.

C. Dropbox and other storage websites

Finally, be careful of using file hosting services such as Dropbox for sharing PHI because they are subject to their own security issues. If you use Dropbox or a similar website, be sure that it is HIPAA compliant and provides enhanced security measures such as encryption.

VII. HOW DO I PROTECT MY PRACTICE?

A. Specific protocols for your practice

While the statutes themselves do not provide any specific guidance on how to ensure compliance in your office, there are many companies that have established suggestions of ways an office can ensure compliance and we have a few suggestions of our own. As required by HB 300, the **office training** must be provided to each employee of a covered entity within the first 90 days of his/her employment. Additional training is required if there is a material change to the federal law or state law within one year of the material change. Additionally once trained, the employer must have each employee acknowledge that they received the training by signing electronically or in writing that they received the training and that employer must keep the certification on file for six years. A sample certificate is attached as Form C.

The second thing that all lawyers should implement is have their client's sign an **authorization** (attached as Form A) at the same time the Client is completing the fee agreement. By doing this at the start of your case, you will not run the risk of an unauthorized disclosure.

Additionally, every practitioner should make it a habit to enter into a **Model Business Associate Agreement** (attached as Form B) with each person that will be working on each case. That would include any experts, (financial or psychological), but it could also extend to your IT group that does work on your office computer, the shredding company you use to dispose of your unwanted case materials, and the storage company you use for offsite storage of your old case files.

Obtaining LESS information from clients – How many of us ask clients for complete social security numbers and driver's license numbers without considering the fact that such information is not needed? Change your consultation information sheets to ask for the last 4 digits of those numbers to reduce potential risk of loss of that confidential information. In other words, you can't lose what you don't have.

HIPAA Provision and Fee Agreements – All fee agreements should provide an acknowledgement that your firm is HIPAA compliant and notifying clients of their HIPAA rights.

Place card on Front Desk – While the fee agreement is probably sufficient to meet the HB 300 notice requirement, you might also consider placing a small notice sign on your front desk.

HIPAA Policy Document – A "Client" rights form is a good practice to also incorporate as a required form when you are first hired by a client. The form would indicate the client's rights under the state and federal laws as well as the required procedure for receiving complaints.

HIPAA Release – Consider insisting that the opposing party signs a HIPAA Release Form allowing access to the documents, especially before conducting discovery wherein protected health information might be disclosed.

HIPAA Child Release – Oftentimes these are needed for any case involving custody and you should obtain this release from your client (or other spouse) to maintain child's records for your case. (Attached as Appendices)

Office Locks – If possible, secure the lawyers offices behind your reception area to protect the privacy of the documents in your office.

Shredding Machine – Small electric shredders can be kept under your desk for use when clients are present and want to be absolutely assured that their confidential documents are shredded.

Shred Bin – It is essential that you have a shredding policy for confidential documents. Various HIPAA compliant companies will offer to place shred bin containers in your office for the deposit of confidential documents and pick up those documents on a regular basis.

Computer Passwords – Every office should require that its employees maintain strong passwords for access to your computer system. It is also critical to change those passwords on a regular basis. You should ensure that those passwords are not written down under staffs keyboards or their computers because that defeats the purpose of having them in the first place.

Video Security – If you have storage areas with HIPAA documents, consider video security to enhance your client's privacy.

Encryption – All laptops and other remote computers should be encrypted to protect the computer from wrongful access.

Server Protection – Is your server protected? Your server should be in a separate strongly secured closet or secured room that is not easily accessible.

1. The Application of HIPAA In The "Courtroom"

By now you should know that as an attorney in the state of Texas, you are a covered entity pursuant to the federal and/or state guidelines governing protected health information. As a covered entity you must be extremely cautious when obtaining and disclosing protected health information (PHI).

With the vast majority of contested family law cases involving mental health and/or drug or alcohol abuse issues, chances are that you have or will come in contact with protected health information. It is imperative that you know how to properly obtain and disclose this information throughout your case, as well as how to properly dispose of this information once the case is over. Failure to abide by both the federal and state rules governing the disclosure of PHI can have severe monetary penalties.

This article will outline several common scenarios encountered in family law practice where the need may arise to obtain and disclose protected health information. Next, this article will outline the proper authorizations and/or court orders required to release and disclose protected health information. Additionally, this article will outline the measures that you should take if your client's protected health information is requested. Finally, this article will outline how to exclude protected health information during litigation.

VIII. TAILOR REQUESTS FOR PROTECTED HEALTH INFORMATION (PHI)

Many family law practitioners frequently issue requests for production of documents in a divorce or child custody dispute. It is important to carefully evaluate the issues in your case prior to sending a request for production or other discovery request seeking the release of protected health information. If you do not need the information, do not request it. Once you have protected health information in your possession, as a covered entity, your duty to protect the disclosure of this information is triggered.

If you decide that requesting protected health information in your case is necessary, decide what specific protected health information is needed, and only request the release of that specific information. Limiting the amount of protected health information in your possession reduces the chance of improper disclosure of this information. When tailoring requests for protected health information, you should narrow your requests and only seek to obtain the information that you need in your case. For example, do not send a generic request for, "any and all medical records from any medical providers that a litigant has been treated by for a specific time period." If you do, you are likely to obtain a great deal of protected health information that you are now required to protect, most of which will not be useful or relevant to you in your case.

IX. SECURING A RELEASE AND/OR COURT ORDER TO OBTAIN PROTECTED HEALTH INFORMATION

1. Releases are Required to Obtain and Release Protected Health Information of the Opposing Party as well as your Client

Once you have decided what protected health information is relevant to the case, you now have to determine the best way to obtain an authorization for the release of this information. You can obtain a release, directly from the patient, authorizing you to obtain his/her protected health from the healthcare provider. If obtaining a release directly from the patient is not possible however, then you can obtain a court order compelling the release of protected health information.

Typically, attorneys are aware of the need for a release to obtain the protected health information of the opposing party. However, the same rules apply to the release and disclosure of your own client's protected health information. If your client's protected health information is requested, you must have a valid authorization from your client to disclose his/her information. Therefore, before you send your client's medical records to the other side in response to a request for production or before you use these records in a hearing or trial, you must be sure that you have a valid authorization to do so.

If protected health information is sought from multiple healthcare providers, you must have a separate authorization signed by the patient for each healthcare provider.

2. How to Properly Obtain Protected Health Information - Requirements of a Valid Authorization

The first step to obtaining a valid authorization for the release of protected health information is to be aware of the requirements of a valid authorization. Some of the requirements of a valid authorization are the same under both the federal and state requirements. It is the best course of action to use a single authorization form which complies with both the state and federal requirements.

A valid authorization that complies with both federal and state regulations must:

i. Be in writing;
ii. Be dated and signed by the patient or the patient's legal representative;
iii. Identify the information to be disclosed in a specific and meaningful fashion;
iv. Identify the person(s) or entity(ies) to whom information may be disclosed;
v. Specify each purpose of the requested use or disclosure;
vi. Include an expiration date or expiration event. If no expiration date is desired, the authorization should state that vii. the authorization does not expire; and
viii. The authorization may not be contained in the same document as the patient's consent to medical treatment.

There are many forms of HIPAA authorizations available to practitioners from various sources. Be cautious when obtaining a release from the internet or from other sources. The Office of the Attorney General adopted an approved authorization/release that satisfies the requirements of both the federal and state laws. A copy of this authorization is attached hereto as Appendix A.

It is important to know that certain types of protected health information, such as mental health records and drug and alcohol records, are afforded a greater level of protection than other medical records. You must be sure, if you are seeking these types of records, that your authorization is specific enough to secure the records you really want produced.

3. What if a Party Refuses to Sign an Authorization

Oftentimes, a discovery request seeking the production of protected health information from the opposing party or a healthcare provider will result in a refusal to produce the information. This usually comes in the form of the assertion of a privilege and/or a motion to quash or motion for a protective order. Therefore, it is prudent to send an authorization for the release and disclosure of protected health information to the opposing party when issuing a request for production of documents. If the opposing party refuses to voluntarily execute a proper authorization for the release and disclosure of their protected health information, then you should file a motion to compel the release and disclosure of this information. Obtaining the proper authorization or court order for the release and disclosure of information depends on the type of protected health information you are seeking.

If you file a motion to compel protected health information, you should also request the Court to overrule any objections made to the production of this information. As part of your motion to compel, you should seek an order from the Court requiring the party to execute an authorization for the release of this information. Another alternative is to seek an order from the Court compelling the health care provider to release the information. An example of a court order requiring the healthcare provider to provide this information is attached hereto as Appendix B. It is

recommended to seek both an order from the Court compelling the party to execute the release, as well as an order compelling the healthcare provider to release the information.

X. NOW WHAT? YOU HAVE AN AUTHORIZATION OR COURT ORDER

Once you have a valid authorization and/or court order you should issue a subpoena duces tecum directly to the healthcare provider requesting the protected health information. You should send both the executed authorization and/or the court order to the healthcare provider along with the subpoena.

If you are issuing a third party discovery subpoena, you must comply with all subpoena and notice requirements as outlined in rule 205 of the Texas Rules of Civil Procedure.

1. Drafting a valid Subpoena for Medical Records

1. <u>You Must Comply with the Standard Requirements for a Valid Subpoena Outlined in Texas Rule of Civil Procedure 176.1 as follows:</u>

   i. The subpoena must be issued in the name of The State of Texas;
   ii. State the style of the suit and its cause number;
   iii. State the court in which the suit is pending;
   iv. State the date on which the subpoena is issued;
   v. Identify the person to whom the subpoena is directed;
   vi. State time, place, and nature of the action required by the person to whom the subpoena is directed, as provided in Rule 176.2;
   vii. Identify the party at whose instance the subpoena is issued, and the party's attorney of record, if any;
   viii. State the text of Rule 176.8(a); and
   ix. Be signed by the person issuing the subpoena.

2. <u>You Must Provide Satisfactory Assurance to the Covered Entity with your Subpoena</u>

If you have a court order or subpoena, signed by the presiding judge in your case, then you do not need to provide satisfactory assurances to the covered entity. 45 C.F.R. § 164.512(e)(1)(i). You should be sure to send a copy of the court order to the covered entity along with the subpoena.

If you do <u>not</u> have a court order requiring the release of protected health information to accompany your subpoena, then you must provide satisfactory assurances to the covered entity that the patient has been notified that his/her protected health information has been requested. 45 C.F.R. § 164.512(e).

Satisfactory assurances include the following written statements, which must be provided to the covered entity:

   i. A party requesting such information has made a good faith attempt to provide written notice to the individual;
   ii. Sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court;
   iii. The time for the individual to raise objections have elapsed, and either no objections were filed or any objections have been resolved by the court.

Id. at § 164.512(e)(1)(iii).

XI. USING PROTECTED HEALTH INFORMATION IN YOUR CASE

Now you have the protected health information in your possession, you must be extremely careful not to disclose the information to anyone, unless you have specific authority to do so. Many times, as a case progresses, the players may change. Your initial authorization or court order may only authorize the release of protected health information to you or your firm. Therefore, if it becomes necessary to release this information to any person not covered by your court order or authorization, you must seek a new authorization and court order. For instance, if you subsequently hire an expert witness, or the Court orders a custody evaluation or psychological evaluation, etc., you will need to obtain an authorization and/or court order that enables you to release the information to these individuals.

Additionally, the need may arise to use protected health information when filing pleadings and in court. It may become necessary to file an emergency request for relief or for temporary orders, wherein you need to use protected health information to support your request for relief. You may conduct oral depositions or attend hearings when you need to use protected health information as evidence in the form of exhibits. Before you can disclose this information

to the Court, be sure you have an authorization to do so. This may require you to obtain a new authorization or court order allowing the disclosure of the protected health information to others. Failure to do so is a violation of both the state and federal rules.

A. Common Persons to whom Protected Health Information may Need to be Disclosed in Family Law Cases

1. Your client:

    a. You must have authorization to disclose protected health information of the other party to your client.

2. The Court:

    a. You must have an authorization or court order that authorizes you to disclose protected health information to the Court before you can use it as an exhibit in a final trial or hearing, as support for relief when filing an application of temporary restraining order, application for protective order, and/or other emergency relief.

3. Court-Ordered Experts:

    a. The Court may order a custody evaluation in your case. During the evaluation, it is common for the evaluator to request that each side provide documentation and information to the evaluator. If you plan to provide protected health information to the evaluator, you must have an authorization or court order that allows you to disclose the information to the evaluator.

4. Consulting Experts:

    a. It is common practice for attorneys to consult with experts during a case. If you plan to provide protected health information, you must have an authorization or court order that allows you to disclose the information to the consulting expert.

5. Testifying Experts:

    a. It is common practice for attorneys to retain testifying experts during a case. If you plan to do so, you must have an authorization or court order that allows you to disclose protected health information to the testifying expert.

6. Use During Depositions:

    a. Depositions are conducted in many family law cases. If you plan to conduct depositions and use protected health information as an exhibit, you must have an authorization or court order that allows you to disclose the information during the deposition.

B. Protected Health Information that Most Family Law Practitioners will Encounter

1. Medical Records:

    a. You may come into contact with medical records, which include billing statements during litigation.

2. Mental Health Records:

    a. In many family law cases, it is common to be in possession of mental health records of either your client or the other party. These records may be from counselors, psychologists, psychiatrists, or in-patient or out-patient treatment facilities. Additionally, the Court may order the psychological evaluation of your client and/or the other party wherein a report containing protected health information will be released to you. A copy of a court order authorizing the release of a psychological

evaluation to the attorney and authorizing the disclosure of the evaluation by the attorney to others is attached hereto at Appendix C.

3. Drug and Alcohol Treatment Records:

   a. The need may arise for you to obtain drug and/or alcohol treatment records. It may be extremely difficult for you obtain drug and/or alcohol treatment records. However, the Court should compel the release of these records, if they are relevant to the issues in your case. If you obtain these records, you must have a court order or authorization to release these records to your client or anyone else.
   b. If you know that drug and alcohol treatment records will be needed in your case at the outset, it is best to go ahead and request the records in the early stages of the case. If you know it will be necessary to obtain these types of records during your case, request this relief at your temporary orders hearing or earlier. Incorporate this request for relief in your summary of requested relief exhibit. Be sure that any orders regarding the release and disclosure of this information are included in the order to be signed by the judge.

4. Drug Testing and Monitoring Records:

   a. During your family law case, the Court may order drug and/or alcohol testing and/or monitoring. These results will likely be released to you. Before you release these records to your client or anyone else, you must be sure that you have an executed authorization or court order that allows you to disclose these records and information.
   b. When dealing with drug and alcohol testing and monitoring records, you must obtain a court order that requires the results to be released by the testing or monitoring facility to you, as well as a court order that authorizes you to disclose the results to any and all individuals that will need to review or analyze these records during your case. It is best to include a request for these authorizations in your summary of requested relief exhibit at the first hearing in your case. This action could save you from the requirement of a future hearing to acquire the proper authorization to obtain and disclose this information. If you request an order from the Court for the release and disclosure of this information, you must be sure to incorporate the authorization into the court order to be signed by the judge. A copy of a court order authorizing the release of drug testing records by the testing facility to the attorney and the disclosure of the results by the attorney to others is attached hereto at Appendix D.

XII. PROPERLY STORING PROTECTED HEALTH INFORMATION

Once you have protected health information in your possession, you must ensure that any hard copies of these records are stored under lock and key. All filing cabinets containing hard-files with protected health information are required to be locked. You cannot leave working copies of records on your desk, in your car, at your home, etc. Unless you are presently using them, they must be stored away properly.

Many law firms have now gone "paperless", and most case-related documentation is stored electronically. Therefore, you must ensure that all of these records are properly stored on your computer. It is required that you maintain a username and password to access your files. You must also set your computer to time-out after a period of inactivity, requiring a password to re-gain access. You must be sure that anytime you are accessing these types of records via a wireless or other network that the network meets the level of security required to properly protect the improper disclosure of protected health information.

XIII. RELEASING YOUR CLIENT'S PROTECTED HEALTH INFORMATION

You are required to obtain the same authorizations/releases from your own client as you are from the opposing party when dealing with protected health information.

If your client's protected health information is requested you must:

1. Evaluate whether or not the protected health information being requested is relevant to the case. The Court may have to conduct an in-camera inspection of the documents to determine whether or not they are relevant to the case.
2. Assert the proper objections and privileges in response to a request for production of this information, whether or not the requested information is relevant to the case.
3. File a motion to quash if your client's protected health information is being requested by the other party, from a third party healthcare provider.

4. Require that the Court enter an order compelling your client to execute a valid authorization to release the information.
5. Request a protective order from the court to further protect and limit the release and disclosure of your client's protected health information.
6. Confirm that any authorization your client may be ordered to execute, complies with both the federal and state regulations.
7. Make sure that if you are sending protected health information electronically or stored on a disk, flash drive, etc. that you properly protect the information. For example, never send medical records unencrypted via email.
8. If your client's protected health information is admitted into evidence, file a motion requesting that the evidence be sealed and/or that the case file be sealed. This would prevent the information from becoming public record.

XIV. DISPOSING OF PROTECTED HEALTH INFORMATION WHEN THE CASE IS OVER

If a client file in your office contains protected health information, you must properly dispose of the information. In order to properly dispose of protected health information you must either return the protected health information to the patient or you must destroy the information. This includes both paper and electronic copies of the records.

XV. TIPS FOR OBTAINING AND USING PROTECTED HEALTH INFORMATION:

1. Analyze the need to obtain the protected health information of a party at the outset of your case. As soon as you realize you need this type of information you should take the action necessary to obtain an authorization for this information.
2. Request an authorization and/or court order for the release of protected health information as early as possible. This can eliminate the need for future hearings to obtain the authorization, which will save time and money.
3. Incorporate your request for authorization for the release of protected health information into your requested relief exhibits for temporary orders.
4. If you know that drug and/or alcohol testing is being requested, incorporate a request for the release of this information into your summary of requested relief exhibit. Do not wait until after the testing is ordered to request an authorization to obtain and release the results.
5. Narrowly tailor any discovery requests seeking the release of protected health information. Do not send out general requests for the production of "any and all medical records." Make your requests for protected health information extremely specific.
6. Send a valid authorization to the other party with any discovery request seeking the release of his/her protected health information.
7. If the other side objects to the request for production of protected health information, file a motion to compel the release of the information and request that the objection(s) be overruled.
   Make sure that everyone within your office/firm that comes into possession of protected health information protects that information from improper disclosure.

XVI. SUMMARY OF OFFICE HIPAA

The expansion of HIPAA through HB 300 in Texas to include lawyers is certainly a new frontier for all of us. Ensuring that we comply with these new regulations is important for the protection of our clients and our practices.

XVII. FORMS

a. HIPAA AUTHORIZATION
b. HIPAA RELEASE (CUSTOM)
c. HIPAA RELEASE FOR A CHILD
d. BUSINESS ASSOCIATE AGREEMENT
e. HIPAA TRAINING ACKNOWLEDGEMENT
f. HIPAA FEE AGREEMENT LANGUAGE (SUGGESTED)
g. MOTION FOR ORDER TO OBTAIN PROTECTED HEALTH INFORMATION
h. ORDER TO RELEASE AND DISCLOSE PROTECTED HEALTH INFORMATION BY MENTAL HEALTH EXPERT
i. ORDER TO RELEASE AND DISCLOSE HEALTH INFORMATION BY FORENSIC TESTING LAB
j. COMPREHENSIVE ORDER TO RELEASE AND DISCLOSE PROTECTED HEALTH INFORMATION BY ATTORNEYS AND MENTAL HEALTH EXPERTS