UNT DALLAS COLLEGE *of* LAW

ON • THE • CUSP

LAW REVIEW 2018–2019

ARTICLE

HOT TOPICS IN HIPAA COMPLIANCE

SCOTT CHASE[1]

Table of Contents

Introduction

On August 21, 1996, the federal Health Insurance Portability and Accountability Act ("HIPAA") was signed into law.[2] Among its several reasons, it was created to "improve the portability and accountability of health insurance coverage."[3] "Portability" was to ensure health insurance coverage for employees between jobs.[4] Accountability was meant to ensure the security and privacy/confidentiality of all patient information/data, regardless of insurance status.[5] This private patient information is known as "protected health

---

[1] Scott Chase is a partner at Farrow-Gillespie Heath Witter, and has been Board Certified in Health Law by the Texas Board of Legal Specialization since 2002. He holds a B.A. Political Science and a J.D., both from University of Houston. Tahlia Clement is a law clerk at Farrow-Gillespie Heath Witter. Tahlia is a 2019 candidate for a Juris Doctor at SMU Dedman School of Law, where she is the Editor-in-Chief for SMU's Science and Technology Law Review. She holds a B.A. in journalism and mass communications from Arizona State University.

[2] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified primarily in Titles 18, 26, and 42 U.S.C.).

[3] *Id.*

[4] *See* Celeste L. Toy, *Legislative Analyst's Office*, 17-WTR Cal. Reg. L. Rep., 381, 382 (2001).

[5] *Id.*

information" ("PHI").

Regulations developed by the federal Department of Health and Human Services ("HHS") relating to accountability resulted in uniform standards for security and confidentiality of PHI, and for electronic transmission of PHI and patient financial information.[6] Those accountability procedures became a vehicle to encourage the healthcare industry to computerize patients' medical records and eventually led to a 2009 update of HIPAA, known as the Health Information Technology for Economic and Clinical Health Act ("HITECH").[7]

This article is not meant to be a primer on HIPAA or HITECH compliance, but rather to alert all attorneys, particularly health law practitioners, to timely "hot topics" in such compliance.

I. Data Breaches.

As the use and transmission of electronic medical records on portable devices becomes more prevalent, so do the risks of data breaches.[8] HIPAA provides for fines to be levied for breaches, but recent enforcement actions show that large, multi-million dollar fines for other compliance lapses, such as a lack of security audits or a failure to take corrective actions after breaches are discovered, can be levied.[9]

For example, in 2017, HHS levied a $3.2 million fine against Children's Medical Center of Dallas ("Children's") over uncorrected privacy and security breaches dating back to 2007.[10] In 2010, Children's reported that "personal information for about 3,800 patients had been accessible on an unencrypted, non-password protected" cell phone used at the Dallas-Fort Worth International Airport.[11] The subsequent investigation found that Children's was aware of that type of risk since at least 2007, and that during 2007 and 2008, Children's had

---

[6] Health Insurance Portability and Accountability Act, 110 Stat. at 104-191.

[7] 2009 Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 227 (2009).

[8] Reid Cushman et al., *Ethical, Legal, and Social Issues for Personal Health Records and Applications*, 43 J. BIOMEDICAL INFORMATICS S51, S52 (2010).

[9] *See* U.S. DEP'T OF HEALTH & HUM. SERVS., ENFORCEMENT HIGHLIGHTS (2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/2017-february/index.html.

[10] Sabriya Rice, *Children's Dallas Docked $3.2 Million Over Patient Privacy Breaches*, DALLAS NEWS (Feb. 2, 2017), https://www.dallasnews.com/business/health-care/2017/02/02/childrens-dallas-docked-32-million-patient-privacy-breaches.

[11] *Id.*

various consulting firms conduct analyses regarding its PHI security.[12] Although those firms recommended encryption as a high priority, Children's did not implement encryption on "laptops, workstations and other devices distributed to the Children's workforce until April 2013."[13] In April 2013, a laptop was stolen that contained unencrypted PHI for nearly 2,500 people, which Children's reported three months later.[14] Though Children's voluntarily reported potential disclosures of thousands of patients' PHI, HHS found that Children's had not implemented strong safeguards in a timely manner to ensure the breach would not happen again.[15] Thus, the $3.2 million fine.[16]

Another example shows the need to comply with all the provisions of HIPAA: a delay in notifying patients that their PHI was possibly exposed could result in a fine as well. In October 2015, an unauthorized individual accessed a website maintained by CoPilot Provider Support Services ("CoPilot").[17] That individual gained access and downloaded PHI of more than 220,000 patients.[18] Though the incident was resolved, CoPilot delayed issuing breach notifications until January 2017.[19] That delay resulted in a $130,000 fine levied upon CoPilot.[20]

Now, although it has been two years since the breach and eight months since notifications were issued, 653 patients of a Texas orthopedic clinic are just discovering they have been impacted.[21] While this delay has been considerable, the affected patients have been offered identity theft protection services without charge for twelve months.[22] The Texas orthopedic clinic is still at risk for a fine from HHS due to the unreasonable delay.[23]

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *See id.*

[16] *Id.*

[17] *See* Jessica *Davis, CoPilot Settles with New York AG for Delaying Breach Notification One Year*, Healthcare IT News (June 16, 2017, 1:03 p.m.), https://www.healthcareitnews.com/news/copilot-settles-new-york-ag-delaying-breach-notification-one-year.

[18] *See id*.

[19] *See id*.

[20] *See id*.

[21] *See id*.

[22] *See id.*

[23] *See* Davis, *supra* Note **Error! Bookmark not defined.**.

Medical facilities, large and small, need to be aware that a breach of PHI may lead to HHS investigation of all security policies.[24] In fact, so far in 2018 there have already been over 229 data breaches reported to HHS.[25] Encryption and constant monitoring of any electronic device that can store or access PHI are recommended, as are timely remedial steps when a breach is discovered.[26]

II. Effect of Texas Medical Privacy Law

HIPAA defines a "covered entity" as any healthcare provider, healthcare clearing house, and health plan.[27] Further, HIPAA defines "business associate" as a person or entity other than a member of a covered entity who performs activities for a covered entity that provides that person or entity access to PHI.[28] The Texas Medical Privacy Act defines a "covered entity" as "any person who…comes into possession of protected health information."[29] Texas's definition is much broader than HIPAA and covers a variety of professionals as a "covered entity."[30]

Texas attorneys are now considered a "covered entity" under the Texas Medical Privacy Act ("TMPA") when an attorney obtains patient medical records in a professional capacity.[31] This law has added various provisions that require Texas covered entities to change routine business practices, as described below.[32]

First, covered entities are required to provide a training program to their employees regarding state and federal medical privacy laws, as they relate to the entity's course of business and each employee's scope of employment.[33] Because

---

[24] *See* Office of Civil Rights, U.S. Dep't of Health & Human Serv., Enforcement Highlights (2017).

[25] *See*, Julie Spitzer, *6.1M healthcare data breach victims in 2018*, Becker's Health IT & CIO Report (Aug. 22, 2018), https://www.beckershospitalreview.com/cybersecurity/6-1m-healthcare-data-breach-victims-in-2018-5-of-the-biggest-breaches-so-far.html.

[26] Lucy L. Thomson, *Health Care Data Breaches and Information Security: Addressing Threats and Risks to Patient Data*, *in* HEALTHCARE IT: THE ESSENTIAL LAWYER'S GUIDE TO HEALTH CARE INFORMATION TECHNOLOGY AND THE LAW 253, 256 (Arthur Peabody, Jr. ed., 2013).

[27] 45 C.F.R. § 160.103 (2018).

[28] *Id.*

[29] TEX. HEALTH & SAFETY CODE ANN. § 181.001.

[30] *See id.*

[31] *See* Peg D. Hall & Matt Nickel, *New Medical Privacy Law in Texas: What You Need to Know*, Dallas Bar Association (July 24, 2015, 12:32 p.m.), http://www.dallasbar.org/book-page/new-medical-privacy-law-texas-what-you-need-know.

[32] *See id.*

[33] TEX. HEALTH & SAFETY CODE ANN. § 181.101.

of this, a training program must be conducted at those firms, or for the attorneys who handle PHI, that explains the updates to the Texas Medical Privacy Act and updates to HIPAA.[34] This training program should also include how employees should access and handle PHI digitally, such as protecting their electronic devices, never sending unencrypted medical information via email, and de-identifying or redacting as much PHI as they can, as soon as they can.[35]

Second, covered entities must provide notice to any individual for whom the entity creates or receives PHI, if the individual's information is subject to electronic disclosure.[36] However, this disclosure is not generally required for purposes of treatment, payment, health care operations, or performing certain insurance or health care maintenance organization functions, all of which would generally be the reason an attorney would disclose PHI.[37] The notice, which is required regardless of any disclosure requirement, can be posted at the firm's place of business, on its website, or any other conspicuous place where the patients are likely to see the notice.[38] Therefore, even if a law firm will be disclosing PHI appropriately but electronically, this notice must be posted.[39]

Finally, covered entities must be aware of the updates to Texas breach-notification laws.[40] Prior to the TMPA, any person who conducted business in Texas and owned or licensed computerized data that included sensitive personal information was required to disclose any breach to any Texas resident whose personal information was or could have been compromised.[41] Now, a covered entity must disclose any breach to any individual whose personal information was or could have been compromised.[42] So, a Texas law firm must now notify any individual if a breach occurs and that individual's personal information was compromised, not just Texas residents.[43]

---

[34] *See id.*

[35] *Id.*

[36] *Id.* at § 181.154.

[37] *Id*.

[38] *Id.*

[39] *Id.*

[40] *See* Act of June 17, 2011, 82d Leg., R.S., H.B. 300 (codified as an amendment to TEX. HEALTH & SAFETY CODE ANN. § 181.101).

[41] TEX. BUS. & COM. CODE ANN. § 521.053(b).

[42] *See* Act of June 17, 2011, 82d Leg., R.S., H.B. 300 (codified as an amendment to TEX. HEALTH & SAFETY CODE ANN. § 181.101).

[43] *See id.*

Because the TMPA is so new, there has not been much guidance from the courts on how exactly this will affect Texas attorneys. However, complaints may be filed with the Texas Attorney General, and we may see that remedy being used in the future.[44]

III. Aetna Case.

Aetna is being accused of breaching the privacy rights of approximately 12,000 beneficiaries by mailing an envelope with a large window that revealed that the contents related to HIV prescriptions.[45] One of HIPAA's primary provisions is that disclosure of PHI may only be made with the "minimum necessary" information to fulfill the purpose of the disclosure.[46] Obviously, describing the HIV condition through the window of the envelope is more than "minimum necessary" to communicate with the insured.[47]

Even though HIPAA does not provide for individual causes of action, a class action lawsuit was filed in Pennsylvania alleging a HIPAA violation.[48] Will this suit affect private causes of actions under HIPAA?

That class action lawsuit alleges that Aetna has a long history with not complying with HIPAA, specifically in regards to HIV privacy.[49] It states that in 2014 and 2015, Aetna was sued in two separate class action lawsuits that both alleged that Aetna jeopardized the privacy of people taking HIV medications by requiring patients to receive the medications through the mail and not allowing them to pick up the medications in person.[50] Those two cases were settled with the condition that Aetna would send a notice to all its insured who had to mail-order their HIV medications that they may now pick up the medication in person.[51]

Aetna then provided the contact information for approximately 12,000 people to a third- party mailing vendor to process the mailing.[52] However, in the

---

[44] TEX. HEALTH & SAFETY CODE ANN. § 181.201.

[45] Class Action Compl. at 2, Beckett v. Aetna, Inc., No. 2:17-CV-03864 (E.D. Pa. Aug. 28, 2017).

[46] 45 C.F.R § 164.502(b), § 164.514(d) (2018).

[47] *See* Class Action Compl., *supra* note 45, at 2.

[48] *Id.* at 7.

[49] *Id.* at 1.

[50] *Id.* at 2.

[51] *Id.*

[52] *Id.* at 8.

course of sending out the notices, Aetna sent them in an envelope with a large transparent window.[53] From the outside of the window, instructions on how individuals could obtain their HIV medications were visible.[54]

In addition to alleging a HIPAA violation, the suit alleges that the insureds did not get the "benefit of the bargain," i.e., their insurance premiums were supposed to pay for the security of PHI.[55] However, this suit has since settled for $17 million.[56] While there is no private cause of action for a HIPAA violation, egregious violations of HIPAA, when coupled with other legal theories, may result in more private litigation.[57]

Conclusion

Practitioners should note that HIPAA breach and cyber-security liability insurance policies are generally available to insureds, either as a separate policy or as a rider to the standard liability policy.[58] Unfortunately, these policies vary in coverage and cost and careful review must be made of these policies to ensure that coverage actually meets the real risk of the insured.[59]

Healthcare privacy is an evolving area of law. With multimillion-dollar fines imposed for a violation of HIPAA, states enacting their own healthcare privacy laws, and entities at risk for class-action lawsuits, it is more important than ever to stay up-to-date with healthcare privacy laws.

---

[53] Compl., *supra* note 7 at 9.

[54] *Id.* at 9–10.

[55] *Id.* at 11, 18.

[56] Jacqueline Howard, *Aetna customers get $17 million in HIV privacy settlement*, CNN (Jan. 17, 2018, https://www.cnn.com/2018/01/17/health/aetna-hiv-privacy-settlement-bn/index.html.

[57] *See* Edward Vishnevetsky, *Can A HIPAA Violation Give Rise To A Private Cause of Action?*, D MAGAZINE (May 27, 2014), http://healthcare.dmagazine.com/2014/05/27/can-a-hipaa-violation-give-rise-to-a-private-cause-of-action/.

[58] Scott Godes & Jennifer G. Smith, *Insurance for Cyber Risks: Coverage Under CGL and "Cyber" Policies*, A.B.A. SEC. OF LITIG., at 3 (2012).

[59] *Id.*