Annals of Health Law

Volume 27
Issue 2 *Summer 2018*

Article 8

2018

Remarks on Patient Privacy: Problems, Perspectives, and Opportunities

Stacey A. Tovino

Remarks on Patient Privacy: Problems, Perspectives, and Opportunities

Stacey A. Tovino, J.D. Ph.D.[*]

I. INTRODUCTION

"Thank you so much for the introduction and a very special thank you to the Beazley Institute for Health Law and Policy and the *Annals of Health Law* for the generous opportunity to participate in this symposium. It is such an honor and a pleasure for me to be here not only today but also to have had the opportunity to visit and work with the students, faculty, and staff of the Beazley Institute throughout this fall semester as a visiting faculty member. Thank you so very much for these opportunities and thank you to all of you in the audience for joining us at this symposium today. I would like to address three things, including one problem, one perspective, and one opportunity relating to patient privacy and health information confidentiality. The problem is a practical one, the perspective is an academic one, and the opportunity is career-related.

II. A PROBLEM

Let me begin with a practical problem, which I did not think about too much during the first eighteen years of my practice, while focusing on helping my health industry clients comply with federal and state health-related statutes and regulations, including the HIPAA Privacy Rule.[1]

---

* Judge Jack and Lulu Lehman Professor of Law and Founding Director, Health Law Program, William S. Boyd School of Law, University of Nevada, Las Vegas. I thank Daniel Hamilton, Dean, William S. Boyd School of Law, for his generous financial support of the research project on which this featured address is based. I also thank Nadia Sawicki, Professor of Law and Academic Director, Beazley Institute for Health Law and Policy, Loyola University Chicago School of Law, and the organizers and participants of the Eleventh Annual Beazley Symposium on Health Law and Policy ("Privacy, Big Data, and the Demands of Providing Quality Patient Care") for their comments and suggestions on the ideas presented at the symposium and in these published remarks.

1. The HIPAA Privacy Rule is a set of federal regulations codified at 45 C.F.R. §§ 164.500-.534 that govern covered entities and business associates with respect to their access, use, and disclosure of protected health information (PHI). *See generally,* Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973 (2017) (detailing the history of the HIPAA Privacy Rule, its application to covered entities and business associates, and the Rule's basic use and disclosure requirements); Stacey A. Tovino, *Teaching the HIPAA Privacy Rule*, 61 ST. LOUIS U. L.J.

However, I have thought about this problem more over the last two years as I started taking on pro bono work on behalf of patients, insureds, and other individuals who believe their health-related rights, including their rights under the HIPAA Privacy Rule, have been violated.

The problem is this: Compliance and industry-side attorneys feel like there is significant regulation of the health care industry and that compliance with all of the different federal and state health-related statutes and regulations can be very difficult and sometimes even overwhelming.[2] However, some patients, insureds, and other individuals are still unable to enforce their basic privacy and confidentiality rights due to a lack of timely remedies.[3] I would like to highlight a few factors that I believe contribute to this practical problem.

First, the HIPAA Privacy Rule does not contain a private right of action for any individual who believes the Privacy Rule has been violated.[4] Under the HIPAA Administrative Simplification regulations,[5] an aggrieved party may only complain about a suspected violation of the HIPAA Privacy Rule to the covered entity itself,[6] the Secretary of the federal Department of Health and Human Services ("HHS"),[7] or a state Attorney General ("SAG") who has the authority under the Health Information for Technology and Economic Clinical Health ("HITECH") Act to bring a civil action seeking damages or an injunction on behalf of a state resident.[8]

---

469 (2017); Stacey A. Tovino, *Complying with the HIPAA Privacy Rule: Problems and Perspectives*, 1 LOY. U. CHI. J. REG. COMPLIANCE 23 (2016).

2. *See, e.g.,* Robert I. Field, *Why is Health Care Regulation So Complex*?, 33 PHARMACY & THERAPEUTICS 607, 607 (2008) (discussing the overwhelming and complex nature of healthcare regulations).

3. *See generally,* Stacey A. Tovino, *A Timely Right to Privacy*, 103 IOWA L. REV. (forthcoming 2018) (analyzing in detail the remedies available to persons injured by violations of the HIPAA Privacy Rule and proposing new federal regulations that would assist in the provision of more timely remedies).

4. *See, e.g.*, Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006) ("We hold there is no private cause of action under HIPAA."); Univ. of Colo. Hosp. Auth. v. Denver Pub. Co., 340 F. Supp. 2d 1142, 1144–46 (D. Colo. 2004) (citing a number of cases and secondary authorities supporting the principle that the HIPAA Privacy Rule does not contain a private cause of action).

5. The HIPAA Administrative Simplification Regulations are codified at 45 C.F.R. §§ 160, 162, 164 (2018).

6. *See* 45 C.F.R. § 164.530(d)(1) (2018) (requiring covered entities to provide a process for individuals to complain about suspected violations of the HIPAA Privacy Rule and/or the covered entity's privacy policies and procedures).

7. *See* 45 C.F.R. § 160.306(a) (2018) (giving persons who believe that a covered entity or a business associate has violated the HIPAA Privacy Rule a right to file a complaint with the Secretary of HHS).

8. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, § 13410(e) (Feb. 17, 2009) [hereinafter, ARRA] (permitting a state attorney general to bring a civil action on behalf of residents of that state to enjoin further violations of the HIPAA Privacy Rule, or to obtain damages on behalf of state residents for violations of the

Through my pro bono work, I have filed many complaints with covered entities, HHS, and SAGs on behalf of patients, insureds, and other individuals who believe their rights under the HIPAA Privacy Rule were violated. In my experience, these complaints have little effect. In terms of my complaints to covered entities, the covered entities either did not acknowledge receipt of my complaint, did not discuss with me or my client the content of our complaint, and/or did not resolve our complaint. In terms of my complaints to HHS, HHS did send me automated email receipts confirming HHS's receipt of my complaints[9] and, sometime later, letters stating that they accepted my complaints for investigation. Perhaps due to the high volume of complaints sent to HHS, HHS has yet to resolve any of my complaints and my clients' HIPAA Privacy Rights continue to be violated.

To date, I understand that HHS has received more than 167,321 complaints alleging non-compliance with the different HIPAA Administrative Simplification Regulations ("HIPAA Rules").[10] After receiving a complaint, HHS determines whether the complaint involves a covered entity or business associate regulated by the HIPAA Rules.[11] If so, HHS may conduct outreach and education, and foster voluntary compliance by the covered entity or business associate with the HIPAA Rules.[12] HHS also may enter into a resolution agreement with, or impose civil money penalties ("CMPs") on, the covered entity.[13] To date, HHS has entered into fifty-two resolution

---

HIPAA Privacy Rule).

9. For example, Automated Email Response re: Complaint No. 127XXXXX I received stated:

> Thank you for filing a complaint via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your complaint. Your complaint will be assigned to an OCR staff member for review and appropriate action. If OCR has any questions about the complaint you submitted, we will contact you directly. Otherwise, you will receive a written response indicating whether or not OCR has accepted your complaint for investigation.

10. *See* U.S. DEP'T HEALTH & HUMAN SERVS., Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (last updated Jan. 17, 2018) ("Since the compliance date of the Privacy Rule in April 2003, OCR has received over 167,321 HIPAA complaints and has initiated over 857 compliance reviews. We have resolved ninety-seven percent of these cases (162,564).").

11. *See, e.g.*, U.S. DEP'T HEALTH & HUMAN SERVS., Health Information Privacy, Enforcement Process, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html (last updated June 7, 2017).

12. *See id.* ("OCR enforces the Privacy and Security Rules . . . by investigating complaints filed with it, conducting compliance reviews to determine if covered entities are in compliance, and performing education and outreach to foster compliance with the Rules' requirements."); *Id.* (stating in a chart that OCR resolves complaints in part by obtaining voluntary compliance, corrective action, or other agreement).

13. *See* Resolution Agreement between U.S. Dep't Health & Human Servs. and Complete P.T., Pool & Land Physical Therapy, Inc. (Feb. 2, 2016).

agreements for HIPAA-related incidents, including settlement amounts as low as $25,000[14] and as high as $5.55 million.[15] In addition, HHS has imposed CMPs on three HIPAA covered entities following formal findings of violations of the HIPAA Rules.[16]

In the beginning, HHS resolved incidents involving allegations of violations of the HIPAA rules relatively quickly via resolution agreements. For example, HHS entered into its first-ever resolution agreement with Seattle-based Providence Health & Services ("Providence") on July 15, 2008, almost three years after the first privacy incident occurred on September 29, 2005, which initially gave rise to HHS's investigation of Providence.[17]

However, cases that result in CMPs take significantly longer to resolve. In the two most recent CMP cases, the length of time between the first complained-about incident and the notice of final penalty determination spanned over seven years.[18] HHS's imposition of a CMP against Lincare took approximately seven years and four months from the date of the very first privacy incident that gave rise to Lincare's investigation.[19] Moreover, HHS's imposition of a CMP against Children's Medical Center of Dallas (Children's) took about seven years and two months from the date of the very first privacy incident that gave rise to Children's investigation.[20]

---

14. *Id.* at 2, ¶ 6 (setting forth a resolution amount of $25,000).

15. *See* Resolution Agreement between U.S. Dep't Health & Human Servs. and Advocate Health Care Network (July 8, 2016), at 3, ¶6 [hereinafter, Resolution Agreement with Advocate Health Care] (setting forth a resolution amount of $5.55 million).

16. *See* U.S. Dep't Health & Human Servs., Notice of Final Determination re: Children's Medical Center (Jan. 18, 2017) (imposing a $3,217,000 CMP on Children's Medical Center of Dallas) [hereinafter, CMC Final Determination]; U.S. Dep't Health & Human Servs., Notice of Final Determination re: Lincare, Inc. d/b/a United Medical (Mar. 1, 2016) (imposing a $239,800 CMP against Lincare) [hereinafter, Lincare Final Determination]; U.S. Dep't Health & Human Servs., Notice of Final Penalty Determination re: Cignet Health Center (Feb. 4, 2011) (imposing a $4,351,600 CMP against Cignet).

17. *See* Resolution Agreement between U.S. Dep't Health & Human Servs. and Providence Health & Servs. (July 8, 2015), at 10 (setting forth a full execution date of July 15, 2008); *Id.* at 1 (noting that laptops containing ePHI were left unattended and were stolen from workforce members of Providence Health & Services on September 29, 2005).

18. *See* CMC Final Determination, *supra* note 16 (receiving complaint in January 2010 and concluding in a final decision in January 2017); Lincare Final Determination, *supra* note 16 (receiving complaint in December 2008 and concluding in a final decision in March 2016).

19. *Compare* Lincare Final Determination, *supra* note 16 (setting forth a final execution date of March 1, 2016); and U.S. Dep't Health & Human Servs., Notice of Proposed Determination against Lincare, Inc. (Jan. 28, 2014), at 2, ¶ 5 (noting that complainant stated he found PHI "under a bed and in a kitchen drawer in approximately November 2008").

20. *Compare* CMC Final Determination, *supra* note 16 (setting forth a final execution date of January 18, 2017); and U.S. Dep't Health & Human Servs., Notice of Proposed Determination re: Children's Medical Center, at 2, ¶ 4 (Sept. 30, 2016) (noting Children's Medical Center's loss of an unencrypted, non-password protected BlackBerry device at the

The two-to-seven-year time frames associated with the resolution agreements and CMP cases are consistent with my and my law colleagues' experiences representing patients who have filed complaints with HHS. Years go by while HHS processes the complaint and conducts an investigation, during which time our clients feel as if nothing is being done and the offending conduct continues. It would be less worrisome if the underlying HIPAA Privacy Rule violations involved one-time, accidental incidents that the covered entity or business associate corrected and/or for which the covered entity or business associate apologized. The problem is that most of my clients are victims of intentional, flagrant, ongoing, and/or repeated violations of the HIPAA Privacy Rule. Even when HHS informs the offending entities that they are under investigation for these violations, it is as if these entities know that the government will do nothing for years, if the government ever does something. Perhaps, as a result, the intentional violations continue. As a former litigator who used litigation as a tool to stop unlawful conduct, it is my belief that the lack of a private cause of action under HIPAA interferes with an injured party's ability to timely enforce his or her right to privacy.[21]

Other factors also interfere with the timely enforcement of rights under the HIPAA Privacy Rule.[22] For example, HHS continues to delay issuing regulations that would allow persons harmed by violations of the HIPAA Privacy Rule to receive a percentage of any settlement or penalty.[23] As background, President Obama directed HHS to issue regulations within three years of HITECH's enactment establishing a process by which persons harmed by violations of the HIPAA Privacy Rule could receive a percentage of any settlement or CMP.[24] To date, HHS has yet to publish these regulations that were due on February 17, 2012, more than six years ago.[25]

Attorneys who represent patients, insureds, and other individuals whose privacy rights have been violated, including myself, have been frustrated by HHS's extreme regulatory delay. These regulations would not only allow but

---

Dallas/Fort Worth International Airport on November 19, 2009).

21. *See* Tovino, *supra* note 3 (justifying and proposing new federal regulations that would offer patients injured by HIPAA Privacy Rule violations a private right of action).

22. *See id.* (thoroughly addressing several factors that contribute to patients' inability to enforce their rights to privacy).

23. *See id.* (providing detail about HHS's failure to issue regulations, required by HITECH, governing the sharing of settlements and penalties with individuals harmed by violations of the HIPAA Privacy Rule).

24. *See* ARRA, *supra* note 8, § 13404(c)(3) ("Not later than 3 years after the date of the enactment of this title, the Secretary shall establish by regulation . . . a methodology under which an individual who is harmed by an act that constitutes an offense . . . may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.").

25. *See id.*

also encourage injured parties and/or their attorneys to do the legwork necessary to prove a violation of the HIPAA Privacy Rule, which could help reduce the time frames for enforcement of privacy rights.

Still other factors interfere with the timely enforcement of rights under the HIPAA Privacy Rule.[26] For example, most SAGs have not taken President Obama up on his offer presented in HITECH to issue injunctions or impose civil damages on covered entities or business associates who violate the privacy rights of state residents.[27] HITECH authorized SAGs that have reason to believe that one or more state residents has been adversely affected by a violation of the HIPAA Privacy Rule to seek an injunction or to obtain civil damages on behalf of such residents.[28] Research reveals that only seven SAGs—those in Vermont, Connecticut, Massachusetts, New York, New Jersey, Minnesota, and Indiana—have brought actions on behalf of state residents injured by violations of HIPAA.[29] Individuals in other states, including those in which I have worked for most of my career, have been unable to convince their SAGSs to follow suit.[30] In all of the pro bono cases in which I have been involved, I have filed complaints with not only the offending covered entities and HHS, but also with the appropriate SAG. To date, I have not received a single response from a SAG with reference to a HIPAA Privacy Rule complaint.

Elsewhere, I thoroughly reviewed a number of additional factors that I believe contribute to the lack of timely HIPAA remedies and encouraged HHS to incorporate more timely remedies into the different HIPAA Rules, including a private right of action, a process for qui tam relators, and government authority to remove the Medicare-participating status of an offending covered entity.[31] By way of analogy, federal regulations governing Medicare-participating facilities that pose an immediate jeopardy to a Medicare beneficiary's physical health or safety state that such facilities can lose their Medicare provider agreements within twenty-three days or have a

26. *See generally* Tovino, *supra* note 3 (addressing several factors that contribute to patients' inability to enforce their rights to privacy).

27. *See infra* notes 28–29.

28. *See* ARRA, *supra* note 8, § 13410(e)(1) ("[I]n any case in which the attorney general of a State has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of this part, the attorney general of the State, as parens patriae, may bring a civil action on behalf of such residents of the State in a district court of the United States of appropriate jurisdiction . . . to enjoin further such violation by the defendant; or . . . to obtain damages on behalf of such residents of the State . . . ").

29. *See* Stacey A. Tovino, Professor, UNLV, *Patient Privacy: Problems, Perspectives, and Opportunities*, Slides 48–53, Nov. 10, 2017 [hereinafter, Tovino PowerPoint] (collecting the actions brought by state attorneys general under section 13410(e) of HITECH).

30. *Id.*

31. *See* Tovino, *supra* note 3 (describing these proposals in more detail).

temporary manager appointed.[32] In my private practice in Houston, Texas, where I worked with health industry clients, I frequently helped my Medicare-participating providers respond to these twenty-three-day termination and manager threats from the federal government. I assisted my clients in stopping the dangerous conduct and/or removing the dangerous conditions to ensure our clients would not lose their ability to participate in the Medicare Program. It is my experience that the potential loss of federal health care program dollars was a tremendous incentive for my clients to comply with federal regulations. Most health care facilities rely heavily on Medicare and Medicaid reimbursement and consider the loss of such funds a financial death sentence.[33]

III. A PERSPECTIVE

In addition to the practical problem associated with the lack of timely remedies for violations of the HIPAA Privacy Rule, I would also like to say that, from my perspective as an academic, the HIPAA Privacy Rule is not always intellectually satisfying. Allow me to provide three examples that will help illustrate this point.

First, the existing case law is not very rich in terms of its ability to teach students or its ability to further the public's understanding of the HIPAA Privacy Rule. For example, courts still cannot spell HIPAA correctly.[34] To date, approximately 1,381 federal and state cases spell HIPAA with two Ps instead of two As.[35] It may be funny when actor Mindy Kaling jokes about this on *The Mindy Project*, as she did in a humorous episode that aired on October 17, 2017. In that episode, Kaling's character, a New York City-based obstetrician-gynecologist, could not even pronounce the acronym correctly, calling it "HIPPO" instead.[36] It was less funny two weeks later, however, when *The Mindy Project* attempted to address the importance of

32. *See* 42 C.F.R. § 488.410(a) (2017) ("If there is immediate jeopardy to resident health or safety, the State must (and [the Centers for Medicare and Medicaid Services] does) either terminate the provider agreement within 23 calendar days of the last date of the survey or appoint a temporary manager to remove the immediate jeopardy.").

33. *See, e.g.*, Thomas Sullivan, *HHS OIG: Medicare and State Healthcare Programs: Fraud and Abuse—OIG Proposes Revisions to Exclusion Authorities and "Early Reinstatement" for Certain Healthcare Providers*, POL'Y & MED. (May 13, 2014), http://www.policymed.com/2014/05/hhs-oig-medicare-and-state-health-care-programs-fraud-and-abuse-revisions-to-the-office-of-inspector-generals-exclusion.html (last visited May 22, 2018) ("[Office of Inspector General] exercising its exclusion authority is referred to by many as a 'kiss of death' or 'death sentence' due to the fact that Medicare and Medicaid are often vital revenue sources for providers.").

34. *See infra* note 36.

35. Westlaw search of "HIPPA" conducted on December 4, 2017, at 8:37 a.m. Central Time in "All State and Federal" click "cases."

36. *See The Mindy Project*, *The Midwife's Tale* (Oct. 17, 2017) (in which Dr. Mindy Lahiri, played by Mindy Kaling, states, "Because of HIPPO, we think Jody's the father").

confidentiality in the context of a breast cancer diagnosis.[37] In this second episode, Kaling's character pronounced the acronym correctly, but the network still spelled the acronym incorrectly in its closed captioning.[38] As an academic, it is frustrating when you are trying to teach the HIPAA Privacy Rule to your students and you have difficulty finding a federal or state judicial opinion or other material that spells the acronym correctly.

Second, some courts still cannot determine whether certain parties in a litigation are covered entities, even though the analysis requires a simple assessment of whether the litigation involves a health plan, a health care clearinghouse, or a health care provider that transmits health information in electronic form in connection with a standard transaction.[39] The courts do not even try in some cases; instead, they say things like, "It is unclear whether the [defendant is a HIPAA] covered entit[y]."[40] After the first week of teaching my own HIPAA Privacy class, even my first-semester, second-year law students, who have not taken any other health law classes, know how to conduct this simple assessment.[41] As an academic, I find it frustrating that courts continuously punt on very basic HIPAA Privacy issues.

Third, many of the federal and state cases that reference the HIPAA Privacy Rule do not materially address, or otherwise interpret, key provisions about which academics have questions.[42] Because the HIPAA Privacy Rule currently contains no private right of action, a good number of the judicial opinions that reference the HIPAA Privacy Rule are simply orders dismissing the lawsuit due to the lack of a private right of action.[43]

Beaulieu v. Frisbie Memorial Hospital is typical in this regard.[44] In *Beaulieu*, pro se plaintiff Christopher Beaulieu sued Frisbie Memorial Hospital (Hospital), alleging that the Hospital violated the HIPAA Privacy Rule when it disclosed Beaulieu's brother's medical records to Beaulieu without his brother's prior written authorization, causing Beaulieu "a lot of stress and emotional problems."[45] In a very brief judicial opinion, the U.S.

37. *See The Mindy Project, Doctors Without Boundaries* (Oct. 31, 2017) (discussing the confidentiality issues associated with the cancer diagnosis of Annette Castellano).

38. *See id.* (stating via closed captioning that, "HIPPA [sic] prevents me from confirming or denying that").

39. *See, e.g.*, 45 C.F.R. § 160.103 (2017) (defining covered entity to include health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with HIPAA's standard transactions).

40. *See* In re Nat'l Hockey League Players' Concussion Injury Litigation, 120 F. Supp. 3d 942, 953 (D. Minn. 2015) ("It is unclear whether the U.S. Clubs are covered entities.").

41. Syllabus from Stacy Tovino, Professor, Health Information Privacy and Technology, Fall 2017 (on file with author).

42. *See infra* notes 43–45.

43. *See supra* note 4.

44. *See* Beaulieu v. Frisbie Mem'l Hosp., 2012 WL 4857036, *1 (D.N.H. 2012).

45. *Id.*

District Court for the District of New Hampshire stated:

> Beaulieu brings this action under HIPAA and the HIPAA Privacy Rule, neither of which creates a private right of action. . . . Rather, a patient must file a written complaint with the Secretary of Health and Human Services through the Office of Civil Rights. It is then within the Secretary's administrative discretion whether to investigate complaints and conduct compliance reviews to determine whether covered entities are in compliance. . . . Accordingly, Beaulieu has failed to state a viable cause of action for the improper release of his brother's medical records, and the complaint should be dismissed.[46]

I can certainly assign this case, or one of the many other cases just like it, to teach my students that the HIPAA Privacy Rule does not contain a private right of action and that lawsuits like these should be dismissed on the defendant's motion. However, a good number of the published judicial opinions that reference the HIPAA Privacy Rule stand for this same point, making it difficult to find HIPAA cases on other, more substantive and questionable, issues.

Even if a case contains a claim that survives the defendant's motion to dismiss, the claim will tend to be a common-law tort claim,[47] a breach of contract claim,[48] or a constitutional law (First Amendment) claim.[49] Although the tort claims are interesting to me because I happen to teach torts, they are generally unhelpful in terms of teaching or understanding the HIPAA Privacy Rule.[50]

---

46. *Id.* (internal references and citations omitted).

47. *See, e.g.*, R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 724 (W. Va. 2012) (stating common law negligence, outrageous conduct, intentional infliction of emotional distress, negligent infliction of emotional distress, negligent entrustment, breach of confidentiality, and invasion of privacy claims following the plaintiff's discovery that his confidential medical and psychological information had been accessed by the defendant's employees and disclosed by such employees to the plaintiff's estranged wife and the wife's attorney).

48. *See, e.g.*, Byrne v. Avery Ctr. for Obstetrics & Gynecology, 102 A.3d 32, 36 (Conn. 2014) (including a common law breach of contract claim based on the defendant's disclosure of the plaintiff's medical records pursuant to a subpoena without the plaintiff's prior authorization; specifically arguing that the defendant breached its contract with the plaintiff when the defendant "violated its privacy policy by disclosing her protected health information without authorization").

49. *See, e.g.*, Complaint at 12, Adheris, Inc. v. Kathleen Sebelius et al., No, 1:13-cv-01342 (D.D.C. 2013) (seeking injunctive and declaratory relief prohibiting HHS from enforcing the marketing provisions in the HIPAA Privacy Rule that would have restricted Adheris from sending "truthful and socially beneficial communications that encourage people to take their medications as prescribed by their treating [physicians]"; arguing that such provisions violate the First Amendment).

50. An exception exists for negligence per se (NPS) lawsuits in which the plaintiff argues that the HIPAA Privacy Rule establishes the duty of care and that a violation of the HIPAA Privacy Rule establishes breach of that duty for purposes of proving the tort of

In addition, even moving outside the case law and towards the available federal and state agency guidance, as those of us who work in the heavily regulated industries frequently do when we teach, many of the HHS resolution agreements,[51] the CMP cases,[52] and the SAG enforcement actions[53] (collectively, the "administrative materials") are such obvious violations of the HIPAA Privacy Rule that one does not need to know anything about HIPAA to know that they are HIPAA violations! For example, I do not need HIPAA to tell me that a dentist should not be throwing sixty-seven boxes of dental records containing PHI into a public dumpster in Indianapolis.[54] Decades-old dental practice acts require their licensees to maintain the confidentiality of dental records and HIPAA did nothing to change that.[55] I also do not need HIPAA to tell me CVS and Rite-Aid should not be placing pharmacy records in public dumpsters[56] because decades-old pharmacy and pharmacist licensing laws also require licensees to maintain confidentiality.[57]

The administrative materials are very helpful to practitioners in terms of

---

negligence. To the extent these cases allow the HIPAA Privacy Rule to be used to establish NPS, they can be helpful for teaching and understanding the HIPAA Privacy Rule. *Compare* Sheldon v. Kettering Health Network, 40 N.E.3d 661, 672 (Ohio App. 2015) (holding that a federal regulation such as the HIPAA Privacy Rule cannot be used to establish NPS under Ohio law) with I.S. v. Washington Univ., No. 4:11-CV-235, 2011 WL 2433585 (E.D. Mo. 2011) (finding that the HIPAA Privacy Rule may be used to establish NPS under Missouri law).

51. *See* U.S. Dep't Health & Human Servs., Resolution Agreements, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last visited May 22, 2017) (listing all of HHS's resolution agreements).

52. *See supra* note 16 (listing the three CMP cases).

53. *See* Tovino PowerPoint, *supra* note 29 (collecting at slides 48–53 the actions brought by SAGs under section 13410(e) of HITECH).

54. *See, e.g.*, Consent Judgment, State of Indiana v. Joseph Beck, Jan. 5, 2015 (Ind. (Marion) Cir. Ct. 2015) (action by the Indiana Attorney General imposing civil penalties on Joseph Beck, a dentist who discarded more than sixty boxes of medical records containing protected health information in a public dumpster in Indianapolis).

55. *See, e.g.*, TEX. OCC. CODE § 258.102 (West 2016) (Texas Dental Practice Act provision stating that a dental record is confidential and privileged and may not be disclosed unless an exception applies).

56. *See* Resolution Agreement between U.S. Dep't Health & Humans Servs. and CVS Pharmacy, Inc., Dep't of Health & Human Servs. (Jan. 15, 2009), https://www.hhs.gov/sites/default/files/cvsresagrcap.pdf (imposing a $2.25M penalty on CVS after CVS disposed of paper PHI in open dumpsters potentially accessible to non-workforce members of CVS); *See also*, Resolution Agreement between U.S. Dep't Health & Human Servs. and Rite Aid, Dep't of Health & Human Servs. (June 7, 2010), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/riteaidres.pdf (imposing a $1M penalty on Rite Aid after Rite Aid disposed of paper PHI in open dumpsters potentially accessible to non-workforce members of Rite Aid).

57. *See, e.g.*, IND. CODE § 25-26-13-15(a) (2017) ("A pharmacist shall hold in strictest confidence all prescriptions, drug orders, records, and patient information. He may divulge such information only when it is in the best interest of the patient . . .").

understanding and predicting enforcement trends. From an academic perspective, however, the administrative materials present case after case of covered workforce members who allow their unsecured, unencrypted, non-password protected electronic and paper PHI to be placed in public dumpsters, left in unlocked cars, left on the subway, left in boxes on a private driveway, and even left under their beds in their master bedrooms and in their kitchens even after they have moved out of the house.[58] I can certainly assign my students a few of these administrative materials so they can see the types of scenarios that give rise to federal and state enforcement actions. After the third one, however, my students get the point and crave something more intellectually challenging.

Although the available administrative materials are not that intellectually robust, what is robust is the scholarship of my peers and colleagues who write in the area of patient privacy and health information confidentiality, as well as the strategic work of my in-house counsel, outside counsel, and consultant colleagues who help their institutions and clients assess and manage privacy, confidentiality, and security-related risks for a living.[59]

IV. AN OPPORTUNITY

The final point I want to make today is to encourage the students in the audience to take advantage of the tremendous opportunities that are out there right now in terms of privacy-related careers.

Twenty-one years ago, in August of 1996, President Clinton signed the HIPAA statute into law.[60] In August of 1996, I was starting my third and final year of law school. The first proposed rule and the first final HIPAA Privacy

58. *See, e.g.*, Resolution Agreement between U.S. Dep't Health & Human Servs. and Massachusetts General Hospital, Dep't of Health & Human Servs. (Feb. 14, 2011), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/massgeneralracap.pdf (establishing a $1M resolution amount after a Mass General workforce member left on the subway documents including: (1) patient schedules containing names and medical record numbers for a group of 192 patients; and (2) billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis, and name of providers for 66 of those patients); *see also* U.S. Dep't Health & Human Servs., Notice of Proposed Determination re: Lincare, Inc. (Jan. 28, 2014), https://www.hhs.gov/sites/default/files/Lincare_NPD_remediated.pdf (proposing the imposition of a $239,800 CMP following HHS's receipt of a complaint alleging that a Lincare workforce member left the PHI of 278 patients under a bed and in a kitchen drawer in the workforce member's home in approximately November 2008).

59. *See, e.g.*, Jessica Mantel & Renee Knake, *Legal and Ethical Impediments to Data Sharing and Integration Among Medical Legal Partnership Participants*, ANNALS HEALTH L.J. (forthcoming 2018) (thoroughly addressing the confidentiality issued raised by the sharing of protected health information between and among the medical and legal services participants in a medical legal partnership).

60. Health Insurance Portability and Accountability Act, PUB. L. NO. 104-191, 110 Stat. 1936 (Aug. 21, 1996).

Rule were published in the Federal Register in 1999 and 2000, respectively, during my second and third years of my legal practice. I remember a supportive and strategic partner at the law firm that I joined right out of law school telling me that the HIPAA Privacy Rule was going to be a tremendous opportunity to build a niche in health law for myself, and she was right. For the students in the audience today, you have the same wonderful opportunities available to you right now. The enforcement date for the European Union's General Data Protection Regulation ("EU GDPR"), for example, is this May; that is, May 25, 2018.[61] The EU GDPR is to you what the HIPAA Privacy Rule was to me when I was in law school. Like the privacy officer career opportunities available under the HIPAA Privacy Rule, the EU GDPR has created a wealth of data protection officer ("DPO") career opportunities. I encourage all of you to take advantage of these outstanding career opportunities.

Not only are there many available privacy-related career opportunities, but I have also seen during my time as a visiting faculty member at Loyola University Chicago School of Law ("Loyola") during the Fall 2017 semester, how Loyola has given its students the best possible platform from which to seek those jobs. I have never seen a set of JD, LLM, and MJ curricula prepare students so well for careers in privacy, as I have seen here at Loyola. Not only are there a wide range of courses that focus exclusively on privacy issues, such as Health Care Privacy and Security, Health Information Privacy and Technology, European Union Privacy Law, Privacy Program Management, and Privacy Breach Incident Management and Reporting,[62] but privacy issues are carefully and thoughtfully woven throughout Loyola's entire health law curriculum.

In Topics in Long Term Care, for example, Professor John Blum's students learn about the privacy issues raised by cameras in nursing home resident rooms.[63] In Public Health and the Law, Professor Blum's students learn about the privacy and confidentiality implications of the collection and

61. *See* EUROPEAN COMMISSION, REFORM OF EU DATA PROTECTION RULES (last visited May 22, 2018), http://ec.europa.eu/justice/data-protection/reform/indexen.htm ("While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018."); COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL (last visited May 22, 2018), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0043:FIN ("On 25 May 2018, the new EU-wide data protection instrument, the General Data Protection Regulation, ("the Regulation"), will become directly applicable, two years after its adoption and entry into force.").

62. *See, e.g.,* SPRING 2018 ONLINE AND PROLAW COURSE SCHEDULE, *Loyola University Chicago School of Law*, (last visited May 22, 2018) https://www.luc.edu/media/lucedu/law/registrar/pdfs/spring/Tentative%20SP18%20Online%20and%20ProLaw%20Class%20Schedule%20.pdf (listing these courses).

63. *See* Professor John Blum, Syllabus, *Topics in Long Term Care* (Spring 2018).

disclosure of PHI to public health authorities.[64] And in Government Health Policy, Professor Blum's students are immersed in the privacy and confidentiality issues raised by telemedicine.[65]

Similarly, in Introduction to Health Law, Professor Nadia Sawicki's students receive not only an outstanding overview of the HIPAA Privacy Rule, but they also learn about common law theories of privacy, which are important because they are the only theories to which private rights of action attach.[66] In Bioethics Law and Policy, Professor Sawicki immerses students in a range of privacy-related issues, including the privacy-related concerns associated with bio-banking and secondary research uses.[67]

By further example, in Food and Drug Law, Professor Jordan Paradise's students examine privacy concerns raised in the context of clinical trials, including the privacy issues associated with clinical databases.[68] And, as we saw at the recent Wiet Life Sciences Conference co-hosted by Professor Paradise and Professor Cynthia Ho in October 2017,[69] there are so many privacy issues associated with the life sciences, not the least of which is the surreptitious collection and disclosure of identifiable genetic information.[70]

Moreover, in Health Care Compliance, Professor Ryan Meade's students learn how to write the HIPAA policies and procedures that are required by 45 C.F.R. § 164.530.[71] In addition, in Advanced Health Care Compliance, Professor Meade's students learn to write corrective action plans for privacy breaches and implementation plans for Office for Civil Rights resolution agreements.[72]

Students at Loyola not only have the opportunity to learn about privacy through traditional campus and online classes, but they also have the opportunity to work in the Health Justice Project ("HJP"), a medical-legal partnership clinic affiliated with Erie Family Health Center ("EFHC"), a federally qualified health center serving low-income, uninsured, and Medicaid-eligible Chicago residents in west and north Chicago and the northern suburbs.[73] Under the supervision of Professors Kate Mitchell and

64. *See* Professor John Blum, Syllabus, *Public Health and the Law* (Fall 2017).

65. *See* Professor John Blum, Syllabus, *Government Health Policy* (Fall 2017).

66. *See* Professor Nadia Sawicki, Syllabus, *Introduction to Health Law* (Fall 2017).

67. *See* Professor Nadia Sawicki, Syllabus, *Bioethics Law and Policy* (Spring 2018).

68. *See* Professor Jordan Paradise, Syllabus, *Food and Drug Law* (Spring 2018).

69. *See Wiet Life Science Law Scholars Conference*, Loyola University Chicago School of Law, Friday, October 13, 2017, Agenda, at 2, Session 3B ("Genetic Regulation and Ethics") (listing Professor Yaniv Heled discussing the surreptitious collection of genetic information by paparazzi).

70. *See* Professor Jordan Paradise, Syllabus, *Law and the Life Sciences* (Spring 2018).

71. *See* Professor Ryan Meade, Syllabus, *Health Care Compliance* (Fall 2017).

72. *See* Professor Ryan Meade, Syllabus, *Advanced Health Care Compliance* (Fall 2017).

73. *See* HEALTH JUSTICE PROJECT, *Loyola University Chicago School of Law, Beazley*

Ron Hochbaum, HJP students encounter a wide variety of HIPAA issues in the course of their representation of EFHC patients.[74] For example, the HJP students' clients must sign HIPAA-compliant authorizations before the students can obtain the clients' medical records.[75] In addition, the students ponder the extent to which they can share the medical records they receive with other attorneys with whom they collaborate and consult.[76] Loyola also offers a Certificate in Privacy Law, which allows both legal and non-legal professionals to focus and learn as much as possible about privacy law, privacy policy, and privacy practice.[77] Loyola also forged a strong relationship with the International Association of Privacy Professionals.[78]

In summary, there is no better place to receive an education than Loyola if you are interested in a career in patient privacy. I cannot encourage the students in the audience enough to take advantage of the wonderful, privacy-related career opportunities that are out there right now and to use the outstanding educational opportunities here at Loyola to do it.

I would like to conclude by stating that this semester has been the most wonderful career-related opportunity for me. It has been incredible for me to see a law school and a health law program care so much about educating students not just in theory and policy, but also in practice, which is my passion. Thank you so much to Loyola University Chicago School of Law and to the Beazley Institute for Health Law and Policy for having me here this semester and allowing me to see, first hand, how a top health law program is run."

Institute for Health Law and Policy (last visited May 22, 2018) *available at* https://www.luc.edu/law/centers/healthlaw/hjp/index.html.

74. *See* Professor Kate Mitchell, Syllabus, *Health Justice Project* (Fall 2017).

75. *Id.*; *see also* 45 C.F.R. § 164.508 (2017) (discussing uses and disclosures for which an authorization is required under HIPAA).

76. Professor Kate Mitchell, Syllabus, *Health Justice Project* (Fall 2017).

77. *See* CERTIFICATE IN PRIVACY LAW, *Loyola University Chicago School of Law* (last visited May 22, 2018), https://www.luc.edu/law/degrees/certificate-privacy-law/.

78. *See, e.g.*, COLLEGES WITH PRIVACY CURRICULA, *Int'l Ass. Privacy Professionals* (last visited May 22, 2018), https://iapp.org/resources/article/colleges-with-privacy-curricula/ (listed Loyola University Chicago School of Law).