Saint Louis University Law Journal

Volume 61
Number 3 *Teaching Health Law (Spring 2017)*

Article 10

2017

Teaching the HIPAA Privacy Rule

Stacey A. Tovino
University of Nevada, Las Vegas, stacey.tovino@unlv.edu

TEACHING THE HIPAA PRIVACY RULE

STACEY A. TOVINO, J.D., PH.D.*

TABLE OF CONTENTS

* Lehman Professor of Law and 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 this research project. I also thank Jeanne Price (Associate Dean for Academic Affairs and Director, Wiener-Rogers Law Library) for locating many of the sources referenced herein. Finally, I thank the organizers and participants of the September 25, 2016 "Complying with Law: An Interdisciplinary Dialogue" symposium sponsored by the *Loyola Journal of Regulatory Compliance* at Loyola University Chicago School of Law as well as the September 29, 2016 "The New EU Data Protection Regulation: Transnational Enforcement and its Effects on U.S. Businesses" symposium sponsored by the *Seton Hall Law Review* at Seton Hall University School of Law for their comments and feedback on many of the ideas presented in this Article.

INTRODUCTION

Twenty years ago, President Clinton signed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) into law.[1] Over the past two decades, the federal Department of Health and Human Services (HHS) has published several sets of rules[2] implementing the Administrative Simplification provisions within HIPAA[3] as well as the Health Information Technology for Economic and Clinical (HITECH) Act within the American Recovery and Reinvestment Act (ARRA).[4] These rules include, but certainly are not limited to, a final rule published on January 25, 2013, governing the use and disclosure of protected health information by covered entities and their business associates (the Privacy Rule).[5]

Since 2003, I have been teaching one-, two-, and three-credit Privacy Rule classes at law schools across the country. I also have provided continuing education and other training programs on the topic of the Privacy Rule to practicing physicians, dentists, clinical psychologists, social workers, nurses, and other health care professionals, as well as non-lawyer privacy officials and other health industry participants. My goal with this Article is to examine approaches to teaching the Privacy Rule to law and non-law audiences. Through trial and error, I believe I have improved my Privacy Rule teaching since 2003, and I wish to share my pedagogical successes and failures in this Article.

This Article proceeds as follows: Part I summarizes the history of the Privacy Rule, including the many proposed rules, interim final rules, final rules, guidance documents, and resolution agreements published by HHS.[6] Part II reviews the Privacy Rule's theory of and approach to health information confidentiality.[7] Part III discusses my experience teaching the Privacy Rule to both law and non-law audiences.[8]

In part because few judicial opinions interpreting the Privacy Rule are substantively helpful, Part III argues that Privacy Rule teachers may wish to

1. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [hereinafter HIPAA].

2. *See infra* notes 18–33 (referencing several sets of proposed, interim final, and final rules).

3. HIPAA, Title II, Subtitle F, §§ 261–264 [hereinafter Administrative Simplification Provisions].

4. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001–13424, 123 Stat. 115, 226–279 [hereinafter ARRA] (including the Health Information Technology for Economic and Clinical Health (HITECH) Act).

5. Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 164.500–164.534, Part 164, Subpart E (2016) [hereinafter Privacy Rule].

6. *Infra* Part I.

7. *Infra* Part II.

8. *Infra* Part III.

teach fewer cases and focus instead on the principles of health information confidentiality gleaned from the preambles to HHS's rulemakings as well as HHS's guidance documents, resolution agreements, and frequently-asked questions.[9] Part III further suggests that Privacy Rule teachers who train non-law audiences solicit questions in advance and use these questions to illustrate the Privacy Rule's use-and-disclosure requirements, as bird's-eye legal overviews tend to be unhelpful.[10]

I. HISTORY OF THE PRIVACY RULE[11]

As signed into law by President Clinton on August 21, 1996, HIPAA had several purposes, including improving portability and continuity of health insurance coverage in the individual and group markets, combating health care fraud and abuse, promoting the use of medical savings accounts, improving access to long-term care services and insurance coverage, and simplifying the administration of health insurance.[12] The Administrative Simplification Provisions, codified at Subtitle F of Title II of HIPAA,[13] directed HHS to issue regulations protecting the privacy[14] of individually identifiable health

9. *Infra* Part III.

10. *Infra* Part III.

11. I have reviewed the history of and the regulatory approach taken in the Privacy Rule in a number of prior scholarly articles. *See, e.g.*, Stacey A. Tovino, *Hospital Chaplaincy Under the HIPAA Privacy Rule: Health Care or "Just Visiting the Sick?"*, 2 IND. HEALTH L. REV. 51 (2005); STACEY A. TOVINO, *Medical Privacy*, *in* GOVERNING AMERICA: MAJOR DECISIONS OF FEDERAL, STATE, AND LOCAL GOVERNMENTS FROM 1789 TO THE PRESENT 644 (Paul J. Quirk & William Cunion eds. 2011); Stacey A. Tovino, *HIPAA Privacy for Physicians*, 17 PATHOLOGY CASE REV. 160 (2012); Stacey A. Tovino, *Gone Too Far: Federal Regulation of Health Care Attorneys*, 91 OR. L. REV. 813 (2013); Stacey A. Tovino, *Silence Is Golden . . . Except in Health Care Philanthropy*, 48 U. RICH. L. REV. 1157 (2014); Stacey A. Tovino, *Complying with the HIPAA Privacy Rule: Problems and Perspectives*, 1 LOYOLA U. CHI. J. REG. COMPLIANCE 23 (2016). With technical and conforming changes, much of Parts I and II of this Article are reprinted from these prior scholarly articles with my permission.

12. *See* HIPAA, Pub. L. No. 104-191, Preface, 110 Stat. 1936, 1936 ("An Act [t]o amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.").

13. *See* Administrative Simplification Provisions, *supra* note 3.

14. Elsewhere, I defined and distinguished the concepts of privacy and confidentiality for purposes of discussions addressing the legal responsibilities of health industry participants. *See, e.g.*, Stacey A. Tovino, *Functional Neuroimaging Information: A Case for Neuro Exceptionalism?*, 34 FLA. ST. U. L. REV. 415, at Parts III(J), IV, and V (2007). This Article uses the same definitions and distinctions. Privacy refers to an individual's interest in avoiding the unwanted collection by a third party of health or other information about the individual. *Id*. at 442. Confidentiality, on the other hand, refers to the obligation of a health industry participant to

information if Congress failed to enact comprehensive privacy legislation within three years of HIPAA's enactment.[15] When Congress failed to enact privacy legislation by its deadline, HHS incurred the duty to adopt privacy regulations.[16] The original HIPAA statute clarified, however, that any privacy regulations adopted by HHS must be made applicable only to three classes of individuals and institutions: (1) health plans; (2) health care clearinghouses; and (3) health care providers who transmit health information in electronic form in connection with certain standard transactions (collectively, covered entities).[17]

HHS responded. On November 3, 1999,[18] and December 28, 2000,[19] HHS issued a proposed and final privacy rule regulating covered entities' uses and disclosures of protected health information (PHI). On March 27, 2002,[20] and August 14, 2002,[21] HHS issued proposed and final modifications to the Privacy Rule. With the exception of technical corrections and conforming

prevent the unauthorized or otherwise inappropriate use or disclosure of voluntarily given and appropriately gathered health and other information relating to an individual. *Id.* Although the Privacy Rule actually is a health information confidentiality rule—because it sets limits on how health care providers and other covered entities can use and disclose appropriately gathered PHI—I use the phrase "Privacy Rule" and the word "privacy" in this Article because these are the phrases and words selected by HHS and used by the public for the rule and the concepts addressed therein. *See, e.g.*, *The HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/ [https://perma.cc/XNM4-TFRM].

15. *See* Administrative Simplification Provisions, *supra* note 3, at § 264 ("If legislation governing standards with respect to the privacy of individually identifiable health information . . . is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards . . . .").

16. *See id.*

17. § 262(a) ("Any standard adopted under this part shall apply, in whole or in part, to the following persons: (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 referred to in section 1173(a)(1)."). *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,924 (proposed Nov. 3, 1999) [hereinafter 1999 Proposed Rule] (explaining that HHS did not directly regulate any entity that was not a covered entity because it did not have the statutory authority to do so).

18. 1999 Proposed Rule, *supra* note 17, at 59,918.

19. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pt. 160–164) [hereinafter 2000 Final Rule].

20. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (Mar. 27, 2002) (codified at 45 C.F.R. pt. 160–164).

21. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pt. 160–164) [hereinafter 2002 Final Modifications].

amendments,[22] these rules as reconciled remained largely unchanged between 2002 and 2009.

The nature and scope of the legal duties of confidentiality that applied to covered entities and their business associates (BAs)[23] changed significantly more than eight years ago. On February 17, 2009, President Obama signed ARRA into law.[24] Division A, Title XIII of ARRA, better known as HITECH, contained certain provisions requiring HHS to modify some of the information use and disclosure requirements and definitions set forth in the Privacy Rule, adopt new breach notification rules, and amend the civil penalty amounts that may be imposed on covered entities and BAs who violate the Privacy Rule.[25]

Since ARRA's enactment, HHS has issued several sets of proposed rules, interim final rules, final rules, and technical corrections both implementing HITECH's required changes to the Privacy Rule as well as responding to other national health information confidentiality concerns. On August 24, 2009, for example, HHS released an interim final rule implementing HITECH's new breach notification requirements.[26] On October 30, 2009, HHS released an interim final rule implementing HITECH's strengthened enforcement provisions, including strengthened civil monetary penalties that the federal

22. *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, Correction of Effective and Compliance Dates, 66 Fed. Reg. 12,434 (Feb. 26, 2001) (codified at 45 C.F.R. pt. 160–164); Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000, 65 Fed. Reg. 82,944 (Dec. 29, 2000) (codified at 45 C.F.R. pt. 160–164) [hereinafter Technical Corrections I].

23. Business associates (BAs) are defined to include individual and institutions who: (1) on behalf of a covered entity, but other than in the capacity of a member of the workforce of a covered entity, create, receive, maintain, or transmit PHI for a function or activity regulated by the HIPAA Privacy Rule; and (2) provide, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5688 (Jan. 25, 2013) (codified at 45 C.F.R. 160 and 164) (adopting 45 C.F.R. § 160.103 and providing a new definition of business associate) [hereinafter Final Regulations].

24. ARRA, *supra* note 4.

25. *Id.* Elsewhere, I critiqued HITECH's imposition of confidentiality requirements directly on BAs and proposed statutory and regulatory changes to HITECH and the HIPAA Privacy Rule, respectively, that would except a class of BAs, including outside counsel, from the confidentiality obligations imposed on other BAs. *See* Stacey A. Tovino, *Gone Too Far: Federal Regulation of Health Care Attorneys*, 91 OR. L. REV. 813 (2013). Elsewhere, I also critiqued HITECH's loosening of the regulatory provision that governs covered entities' uses and disclosures of protected health information for fundraising purposes. *See* Stacey A. Tovino, *Silence Is Golden . . . Except in Health Care Philanthropy*, 48 U. RICH. L. REV. 1157 (2014). This Article builds on my earlier scholarship focusing on the Privacy Rule.

26. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pt. 160–164).

Office for Civil Rights (OCR) may, for the first time since the enactment of the HIPAA statute, impose directly on BAs who fail to maintain the confidentiality of PHI.[27] On May 31, 2011, HHS released a proposed rule that would modify the HIPAA Privacy Rule's accounting of disclosures requirement.[28] On January 25, 2013, HHS released a final rule modifying the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules in accordance with HITECH (Final Regulations).[29] On June 7, 2013, HHS released technical corrections to the Final Regulations.[30] On September 16, 2013, HHS released a Model Notice of Privacy Practices designed to assist covered entities in complying with the Final Regulations.[31] On February 6, 2014, HHS released a final rule modifying the Privacy Rule to provide individuals with a right to receive their laboratory test results directly from their testing laboratories.[32] On January 6, 2016, HHS released a final rule modifying the Privacy Rule to permit certain covered entities to disclose protected health information to the National Instant Criminal Background Check System such as the identities of individuals who are disqualified from shipping, transporting, possessing, or receiving a firearm.[33] And, as of this writing, HHS is working on a notice of proposed rulemaking (NPRM) that would allow civil money penalties and settlements associated with Privacy Rule violations to be shared with harmed individuals, as required by HITECH.[34]

In addition to its proposed, interim final, and final rulemakings, HHS also has made publicly available forty different resolution agreements. In these agreements, covered entities resolve to comply with the Privacy Rule, report to HHS regarding its compliance with the Privacy Rule, and/or pay a resolution

27. HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (Oct. 30, 2009) (codified at 45 C.F.R. pt. 160).

28. HIPAA Privacy Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31,426 (May 31, 2011) (codified at 45 C.F.R. pt. 164).

29. Final Regulations, *supra* note 23.

30. *See* Technical Corrections to the HIPAA Privacy, Security, and Enforcement Rules, 78 Fed. Reg. 32,464, 32,466 (June 7, 2013) (to be codified at 45 C.F.R. pt. 160–164) [hereinafter Technical Corrections II].

31. *Model Notices of Privacy Practices*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/ [https://perma.cc/57PE-8958] [hereinafter Model Notice].

32. CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports, 79 Fed. Reg. 7290 (Feb. 6, 2014) (codified at 45 C.F.R. pt. 164).

33. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS), 81 Fed. Reg. 382 (Jan. 6, 2016) (to be codified at 45 C.F.R. pt. 164).

34. E-mail from Iliana Peters, U.S. Dep't Health & Human Servs., to Stacey Tovino, University of Nevada, Las Vegas (Sept. 26, 2016, 4:23 A.M. PT) (on file with author).

amount.[35] In a recent resolution agreement released by HHS on September 23, 2016, HHS required Care New England Health System (CNE)—on behalf of eight current covered entities that are under CNE's common ownership or control, including Woman & Infants Hospital of Rhode Island (WIH)—to pay HHS $400,000 and complete a comprehensive correction active plan following WIH's loss of two unencrypted backup tapes containing electronic PHI.[36] In a second recent resolution agreement, executed by HHS and New York Presbyterian Hospital (Hospital) on April 19, 2016, HHS required the Hospital to pay $2.2 million and complete a comprehensive corrective action plan following the Hospital's impermissible disclosure of protected health information to the media as part of a reality television show, and the Hospital's failure to implement privacy-related safeguards.[37]

II. THE PRIVACY RULE'S APPROACH TO HEALTH INFORMATION CONFIDENTIALITY

A brief summary of the Privacy Rule's theory and approach to health information confidentiality is necessary before discussing how best to teach the Privacy Rule to law and non-law audiences. The Privacy Rule strives to balance the interest of individuals in maintaining the confidentiality of their health information and the interest of society in obtaining, using, and disclosing health information to carry out a variety of public and private activities.[38] To this end, the Privacy Rule regulates covered entities' and BAs' uses of, disclosures of, and requests for individually identifiable health information (IIHI)[39] to the extent such information does not constitute: (1) an

35. *Resolution Agreements*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html [https://perma.cc/4TJ8-H77G].

36. *See* Resolution Agreement between U.S. Dep't Health & Human Servs. and Care New England Health Sys. (Sept. 23, 2016), http://www.hhs.gov/sites/default/files/9-14-16-wih-racap-1.pdf [https://perma.cc/4KC5-2WRZ].

37. *See* Resolution Agreement between U.S. Dep't Health & Human Servs. and New York Presbyterian Hosp. (Apr. 19, 2016), http://www.hhs.gov/sites/default/files/NYP%20NYMed%20RACAP%20April%202016%20%28508%29_0.pdf [https://perma.cc/V9FE-YV7R] [hereinafter New York Presbyterian Hospital Resolution Agreement].

38. *See* 2000 Final Rule, *supra* note 19, at 82,464 ("The rule seeks to balance the needs of the individual with the needs of the society."); *id.* at 82,468 ("The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole."); *id.* at 82,472 ("The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule.").

39. The Privacy Rule defines individually identifiable health information (IIHI) as

> [I]information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider,

education record protected under the Family Educational Rights and Privacy Act of 1974 (FERPA); (2) a student treatment record excepted from protection under FERPA; (3) an employment record held by a covered entity in its role as an employer; or (4) individually identifiable health information regarding a person who has been deceased for more than fifty years.[40] The name given by the Privacy Rule to the subset of IIHI described in the previous sentence is protected health information (PHI).[41]

Before using or disclosing PHI, the Privacy Rule requires covered entities and BAs to adhere to one of three different rules—sometimes called the use-and-disclosure rules—depending on the purpose of the information use or disclosure.[42] These rules reflect HHS's desire to appropriately balance the interest of individuals in maintaining the confidentiality of their PHI with a wide range of societal interests in obtaining, using, or disclosing PHI, some of which may have greater societal importance and value than others.[43]

The first rule allows covered entities and BAs to use and disclose PHI with no prior permission from the individual who is the subject of the PHI—but only in certain situations. That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out their own treatment,[44] payment,[45] and health care operations[46] activities,[47] as well as certain public benefit activities.[48]

> health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

45 C.F.R. § 160.103 (2016).

40. *Id.* (defining "protected health information").

41. *Id.* (using the phrase "protected health information").

42. §§ 164.502–164.514 (setting forth the use and disclosure requirements applicable to covered entities and business associates).

43. *See* 2000 Final Rule, *supra* note 19, at 82,464 ("The rule seeks to balance the needs of the individual with the needs of the society."); *id.* at 82,468 ("The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole."); *id.* at 82,472 ("The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule.").

44. The Privacy Rule defines treatment as:

> [T]he provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

45 C.F.R. § 164.501 (2016).

As an example of this first rule, a covered general practitioner (GP) who wishes to consult with a specialist in order to treat a patient may disclose PHI to the specialist and the Privacy Rule does not require the patient to give the GP prior authorization for the disclosure.[49] Likewise, a covered hospital that treats a patient may send a bill to the patient's insurer to obtain payment for hospital services rendered without the patient's prior authorization.[50] Similarly, a teaching physician employed by a covered academic medical center may involve medical students, interns, residents, and fellows in patient care, without prior authorization from the patients who are receiving such care, to enable the students and residents to learn to practice medicine.[51] By still further example, a covered entity that is required by state or other law to disclose PHI to another individual or entity may do so without patient authorization.[52] By final illustrative example, a covered entity may disclose a patient's PHI to a law enforcement officer in certain situations, including when the covered entity suspects that the death of the patient may have resulted from criminal conduct.[53] The theory behind these permitted information uses and disclosures is that treating patients, allowing health care providers to obtain

45. The Privacy Rule defines payment as the activities "undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan" as well as the activities of a "health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id.*

46. The Privacy Rule defines health care operations with respect to a list of activities that are related to a covered entity's covered functions. *Id.* (defining "health care operations"). These activities include, but are not limited to, conducting quality assessment and improvement activities, conducting training programs in which medical and other health care students learn to practice health care under supervision, and arranging for the provision of legal services. *See id.*

47. § 164.506(c)(1) (permitting a covered entity to use or disclose PHI for its own treatment, payment, or health care operations).

48. Covered entities may use and disclose PHI for twelve different public policy activities without the prior written authorization of the individual who is the subject of the information. § 164.512(a)–(l). These public policy activities include, but are not limited to, uses and disclosures required by law, uses and disclosures for public health activities, disclosures for law enforcement activities, uses and disclosures for research, and disclosures for workers' compensation activities. *See* § 164.512(a), (c), (f), (i), (l) (2016).

49. § 164.501 (defining "treatment" to include "consultations between health care providers relating to a patient").

50. *See id.* (defining "payment" to include "the activities undertaken by a health care provider . . . to obtain . . . reimbursement for the provision of health care"); § 164.506(c)(1) (permitting a covered entity to disclose PHI for its own payment activities).

51. *Id.* (defining "health care operations" to include "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers.").

52. *See* § 164.512(a) (allowing covered entities to "use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.").

53. § 164.512(f)(4).

reimbursement for providing health care, training medical students and residents, complying with state law, and alerting law enforcement officers to the suspicion of criminal activity outweigh an individual's interest in maintaining complete confidentiality of his or her PHI.

The first rule requires no prior authorization from the individual who is the subject of the information before the information use or disclosure may occur. Under the second rule, a covered entity may use and disclose an individual's PHI for certain activities, but only if the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure.[54] Because the Privacy Rule allows the covered entity to orally inform the individual of (and capture an oral agreement or oral objection to) a use or disclosure permitted by these provisions, this second rule is sometimes referred to as the "oral permission rule," although a more practical written permission also will suffice.

Under the second rule, a covered entity may conduct five sets of information uses and disclosures once the individual who is the subject of the information has been notified and has either agreed or not objected to the information use or disclosure.[55] These five sets of information uses and disclosures include: (1) certain uses and disclosures of directory information, such as name, location, general condition, and religious affiliation;[56] (2) certain uses and disclosures that would allow other persons to be involved in a patient's care or payment for care;[57] (3) certain uses and disclosures that would help notify, or assist in the notification of, family members, personal representatives, and other persons responsible for the care of the individual of the individual's location, general condition, or death;[58] (4) certain uses and disclosures for disaster relief purposes;[59] and (5) certain disclosures to family members and other persons who were involved in the individual's care or payment for health care prior to the individual's death of PHI that is relevant to that person's involvement.[60]

As an illustration of the second rule, the hospital room number and general condition of a patient (e.g., 'good,' 'fair,' 'poor,' 'stable') who has given his or her permission or who has not expressed an objection may be disclosed to a visitor who requests directory information about that patient.[61] Likewise, a woman in labor who wishes her partner to be present for her labor and delivery

54. § 164.510.
55. *Id.*
56. § 164.510(a).
57. § 164.510(b)(1)(i).
58. § 164.510(b)(1)(ii).
59. § 164.510(b)(4).
60. § 164.510(b)(5).
61. § 164.510(a)(1), (2).

may orally give her permission for her health care providers to involve her partner in her care.[62]

The theory behind requiring at least oral permission for these information uses and disclosures is that the patient has an interest in maintaining the confidentiality of his or her PHI; however, the patient also may have an interest in being visited in the hospital, in obtaining assistance with the patient's health care or payment for health care, and being assisted during a disaster. In addition, the patient's family also may have an interest in visiting the patient in the hospital, assisting the patient with his or her health care and financial needs, and obtaining assistance during a disaster. The required oral permission reflects the individual's interest in maintaining the confidentiality of his or her health information but the lack of a requirement for a formal written authorization reflects HHS's desire to make it easy for the individual to ask for or agree to receive help.

The third rule—a default rule—requires covered entities and BAs to obtain the prior written authorization of the individual who is the subject of the PHI before using or disclosing the individual's PHI in any situation that does not fit under the first or second rule. Stated another way, in the event that a covered entity or BA would like to use or disclose PHI for a purpose that is not treatment, payment, or health care operations, that does not fall within one of twelve public benefit exceptions, that is not allowed with oral permission or without an objection, and that is not otherwise permitted or required by the Privacy Rule, the covered entity must obtain the prior written authorization of the individual who is the subject of the information.[63]

The Privacy Rule specifies the form of the authorization required by the third rule, including certain elements and statements that are designed to place the individual on notice of how the individual's PHI will be used or disclosed.[64] This high level of prior individual permission reflects the value HHS places on an individual's interest in maintaining the confidentiality of his or her PHI compared to other societal interests that are far removed from the core functions of covered entities and BAs, such as a health care provider's interest in selling the patient's information to a tabloid magazine or a health plan's interest in disclosing the patient's information to a marketing company to allow the company to market its products and services to the individual.[65]

62. § 164.510(b)(1)(i).

63. § 164.508(a)(1).

64. § 164.508(c)(1)–(2).

65. *See* 2000 Final Rule, *supra* note 19, at 82,514 ("[C]overed entities must obtain the individual's authorization before using or disclosing protected health information for marketing purposes.").

With this background regarding the Privacy Rule's theory and approach to health information confidentiality, Part III of this Article will discuss methods of teaching the Privacy Rule to law and non-law audiences.

III. TEACHING THE PRIVACY RULE

A. Teaching the Case Law

Since Fall 2003, I have taught a number of law courses based heavily in the common law, including Torts. When teaching Torts, I focus almost exclusively on the hundreds of cases made available by the authors of my assigned casebook.[66] I think these cases are outstanding for helping students understand the intentional torts, negligence, strict liability, products liability, and other tort-based theories of liability, as well as their privileges and defenses. Occasionally, I will supplement these cases with a Restatement provision or a Nevada statute (since I teach at the University of Nevada, Las Vegas), especially if the provision or statute is relevant to an issue under discussion. For example, if I am discussing a case in which a plaintiff sues a defendant for one tort but not a second tort because the statute of limitations has already run on the second tort, I may ask the students to look up the Nevada statute that sets forth the statute of limitations for the second tort.[67] The vast majority of my Torts class discussions, however, focus on theories of liability as well as privileges and defenses to the torts as they are presented in federal and state judicial opinions.

When I first started teaching the Privacy Rule in Fall 2003, I was uncomfortable because I was forced to teach straight from the final rule that was published in the *Federal Register* on December 28, 2000,[68] as well as the final modifications published in the *Federal Register* on August 14, 2002.[69] Because most covered entities did not have to comply with the Privacy Rule until April 14, 2003,[70] there were few published cases, other than statutory and regulatory challenges, before then.[71] Even after April 14, 2003, it took cases

66. *See* VICTOR E. SCHWARTZ, KATHRYN KELLY & DAVID F. PARTLETT, PROSSER, WADE, AND SCHWARTZ'S TORTS: CASES AND MATERIALS (13th ed. 2015).

67. NEV. REV. STAT. § 41A.097(2) (2016) ("[A]n action for injury or death against a provider of health care may not be commenced more than 3 years after the date of injury or 1 year after the plaintiff discovers or through the use of reasonable diligence should have discovered the injury, whichever occurs first, for . . . professional negligence . . . .").

68. *See* 2000 Final Rule, *supra* note 19, at 82,462.

69. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pt. 160–164).

70. *See* 45 C.F.R. § 164.534(a), (b)(1) (2016) (establishing an April 14, 2003 compliance date for covered health care providers and non-small health plans).

71. *See, e.g.*, S.C. Med. Ass'n v. Thompson, 327 F.3d 346, 351–55 (4th Cir. 2003) (declaratory judgment action challenging HIPAA; holding that HIPAA did not impermissibly

involving federal health information confidentiality issues a while to work their way through the courts and to be published as judicial opinions. In addition, because the Privacy Rule contains no private right of action, many of the early judicial opinions simply clarified the lack of such right and dismissed the plaintiffs' claims on that basis.[72] Few substantively helpful judicial opinions assessing the use-and-disclosure requirements codified at 45 C.F.R. §§ 164.502–514, the individual rights provisions codified at 45 C.F.R. §§ 164.520–528, the breach notification requirements codified at 45 C.F.R. §§ 164.400–410, and the administrative requirements codified at 45 C.F.R. § 164.530 were available in the early 2000s for use in class discussions.

As courts began publishing opinions addressing substantive HIPAA Privacy issues, I placed them in my syllabus in the appropriate place. Some of these judicial opinions were helpful in clarifying issues that the Privacy Rule itself did not answer.

For example, remember that the first use-and-disclosure rule discussed in Part II allows covered entities and BAs to use and disclose PHI for their own treatment, payment, and health care operations (TPO) activities without any form of prior permission from the individual who is the subject of the PHI.[73] The regulation that allows these uses and disclosures[74] is frequently referred to as the "TPO rule." Although the Privacy Rule defines the terms treatment, payment, and health care operations,[75] these definitions do not answer every single "Is this TPO?" question I receive from my students.

One illustrative question I have received more than once is whether coerced, sometimes called assisted, treatment received by an individual who is

delegate legislative function, the Privacy Rule was not beyond scope of congressional grant of authority, and that neither HIPAA nor the Privacy Rule was impermissibly vague); Ass'n Am. Physicians & Surgeons, Inc. v. U.S. Dep't Health & Human Servs., 224 F. Supp. 2d 1115, 1118, 1126–27 (S.D. Tex. 2002) (declaratory judgment action against HHS challenging the Privacy Rule as beyond the legislative scope of HIPAA as unconstitutional; holding in part that the Privacy Rule was within the scope of HIPAA).

72. *See, e.g.*, Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1146 (D. Colo. 2004) ("Because I find no such statutory intent in HIPAA, I may not imply a private right of action, and University Hospital's claim under HIPAA should be dismissed."); Agee v. United States, 72 Fed. Cl. 284, 289–90 (Ct. Cl. 2006) ("Accordingly, this Court dismisses Plaintiff's claims concerning violations of HIPAA because the statute does not provide for a private right of action against the Federal Government."); Johnson v. Quander, 370 F. Supp. 2d 79, 100 (D.D.C. 2005) ("Here, the plaintiff challenges, pursuant to the HIPAA, the disclosure of information regarding his DNA . . . [B]ecause no private right of action exists under the HIPAA, this Court does not have subject matter jurisdiction over this claim and it must be dismissed.").

73. 45 C.F.R. § 164.506(c)(1) (2016). *See generally supra* Part II (discussing the Privacy Rule's requirements relating to uses and disclosures of protected health information).

74. *See* § 164.506(c)(1).

75. *See* § 164.501 (2016) (defining "treatment," "payment," and "operations" for purposes of the Privacy Rule).

involuntarily committed under state law falls within the Privacy Rule's definition of treatment. If so, a covered entity, such as a covered hospital or clinic, would be permitted to disclose medical records supporting the severity of the individual's mental health condition to a court that would be ruling on the involuntary commitment or a subsequent involuntary health care provider. The Privacy Rule does not address this issue.[76]

However, in *In re Miguel M.*, the New York Court of Appeals[77] held that the purpose of the treatment rule is to facilitate the sharing of PHI among health care providers working together, not the sharing of PHI by one voluntary health care provider with a second, involuntary one.[78] The court reasoned that, "[d]isclosure for that [involuntary] purpose is a more serious invasion of privacy than, for example, the transmission of medical records from a patient's primary care physician to a specialist—the sort of activity for which the treatment exception seems primarily designed. The treatment exception is inapplicable here."[79] I have included *In re Miguel M.* in my Privacy Rule syllabus since its publication in 2011 because I can use it to illustrate a disclosure of PHI that implicates the TPO rule, to help my students understand the difference between voluntary and involuntary treatment, and to teach the limitations of the otherwise broad range of PHI uses and disclosures allowed under the TPO rule.

In re Miguel M. is substantively helpful for other reasons as well. Because not all my HIPAA Privacy students have taken a course in Public Health Law before enrolling in HIPAA Privacy, they may not understand the difference between public health law, which focuses on legal measures that may help identify, prevent, and ameliorate health risks of a community,[80] and private health law, which focuses on legal authorities that help guide disputes between individual physicians and patients, individual hospitals and particular medical staff members, and health plans and in-network or out-of-network providers, among other individual relationships. I have found that students who lack exposure to principles of public health law frequently are unable to apply the public health exception to the Privacy Rule, which allows covered entities to

76. *See id.* (defining "treatment" as the "provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another" but not clarifying whether the definition is limited to voluntary treatment or whether involuntary treatment is included).

77. *In re* Miguel M., 17 N.Y.3d 37 (N.Y. 2011).

78. *Id.* at 43.

79. *Id.*

80. *See, e.g.*, Lawrence O. Gostin, *A Theory and Definition of Public Health Law*, 10 J. HEALTH CARE L. & POL'Y 1 (2007) (defining public health).

disclose PHI to public health authorities for public health purposes without the prior written authorization of the individuals who are the subject of the PHI.[81]

In re Miguel M. is helpful for teaching students when the public health exception to the Privacy Rule applies. In *In re Miguel M.*, the physician who was petitioning for Miguel's involuntary commitment argued that the disclosure of Miguel's PHI would protect the public health because it would help ensure that Miguel would be involuntarily committed and therefore would not injure or kill anyone else, including members of the public.[82] The New York Court of Appeals disagreed, reasoning that the purpose of the public health exception was to "facilitate government activities that protect large numbers of people from epidemics, environmental hazards, and the like, or that advance public health by accumulating valuable statistical information."[83] The court found that the disclosure of PHI of one particular individual, such as Miguel M., for the purpose of preventing that individual from harming himself or others "effects a very substantial invasion of privacy without the sort of generalized public benefit that would come from, for example, tracing the course of an infectious disease."[84] The court ultimately ruled that the disclosure of Miguel's PHI to the physician who was petitioning for Miguel's involuntary commitment did not come within the scope of the public health exception. I love teaching this case because, in addition to the treatment analysis discussed above, it kills two more birds. That is, it teaches students the difference between public and private health and helps them identify situations when the public health exception to the Privacy Rule does and does not apply.

Unlike *In re Miguel M.*, however, many cases addressing Privacy Rule issues interpret the Rule incorrectly, in my opinion, or pass on ruling on Privacy Rule issues that the courts believe are too difficult to answer. For example, many courts struggle with the most basic of Privacy Rule issues, including determining whether a defendant is a covered entity to whom the Privacy Rule applies. In *In re National Hockey League Players' Concussion Injury Litigation*, for example, the United States District Court for the District of Minnesota was set to analyze whether the National Hockey League (NHL) or any of its member teams were covered entities under the Privacy Rule.[85]

81. *See* 45 C.F.R. § 164.512(b)(1) (2016) ("A covered entity may . . . disclose protected health information . . . to . . . [a] public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions . . . . ").

82. *In re Miguel M.*, 17 N.Y.3d at 42.

83. *Id.* at 42–43.

84. *Id.* at 43.

85. *In re* Nat'l Hockey League Players' Concussion Injury Litig., 120 F. Supp. 3d 942, 953 (D. Minn. 2015) (referencing the question of whether the NHL is a covered entity).

This analysis is simple and requires only asking the following: (1) Whether the teams meet the definition of a health plan by making health insurance available to their hockey players;[86] or (2) Whether the teams meet the definition of a covered health care provider by making sports injury and other health care available to the hockey players and subsequently electronically billing a public or private health care program or plan for such care.[87]

Instead of conducting this straightforward analysis, the court says: "It is unclear whether the [hockey teams] are covered entities."[88] I assigned this opinion, published on July 31, 2015, to my Spring 2016 HIPAA Privacy students because I thought the application of the Privacy Rule to a popular professional sports league would be interesting to my sports- and entertainment-obsessed law students. However, the court's failure to rule on the issue in which my students were most interested—the question of whether NHL teams are covered entities—frustrated them. I will not include the opinion in future syllabi.

B. Teaching the HHS Guidance

In part because of the substantive weakness of much of the Privacy Rule case law, I focus my law-based teaching instead on HHS guidance. This guidance includes, but is certainly not limited to, preambles to all the proposed, interim final, and final rulemakings;[89] separate, formal guidance documents released by HHS on various aspects of the Privacy Rule;[90] hundreds of answers to frequently-asked questions made available by HHS;[91] and dozens of resolution agreements entered into by HHS and a variety of covered entities.[92] I have found the HHS Guidance tremendously helpful in teaching the Privacy Rule to law students. Allow me to provide a few examples of teaching strategies using several different types of HHS Guidance.

The preambles to the proposed, interim final, and final rulemakings are gems for teaching. Members of the public ask questions about the application

86. 45 C.F.R. § 160.103 (2016) (defining health plan).

87. *Id.* (defining health care provider; defining covered entity).

88. *In re Nat'l Hockey League*, 120 F. Supp. 3d at 953.

89. *See, e.g.*, *supra* notes 18–32 (referencing all the proposed, interim final, and final rules implementing section 264 of the HIPAA statute).

90. *See Guidance on Significant Aspects of the Privacy Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/significant-aspects/index.html [https://perma.cc/TJN3-RGME] (providing guidance on seventeen different aspects of the Privacy Rule).

91. *HIPAA FAQs for Professionals*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/faq [https://perma.cc/XM2H-VKBM] (providing answers to hundreds of frequently-asked questions in dozens of categories).

92. *Resolution Agreements*, *supra* note 35 (listing resolution agreements entered into by and between HHS and covered entities starting in July 2008).

of the Privacy Rule that are very similar to the types of questions asked by law students, and HHS responds with its interpretation. I frequently assign my law students portions of the various preambles as reading and ask them questions in class based on HHS's interpretations in these preambles. I do this for two reasons. First, the preambles nicely illustrate the notice-and-comment rulemaking process and allow the students to learn the procedure of administrative law while they are learning the substance of the Privacy Rule. Second, I want to encourage students to consult the preamble for HHS interpretations before issuing their own, unverified Privacy Rule interpretations to clients. As I will show using two examples below, HHS's regulations are frequently unclear and the agency's interpretations are not always expected. These two examples follow.

First, the Privacy Rule allows covered health care providers to use and disclose PHI for their own treatment activities.[93] The Privacy Rule defines a *health care provider*, in relevant part, as "any other person or organization who furnishes, bills, or is paid for *health care* in the normal course of business."[94] The Privacy Rule further defines *health care* as:

> [C]are, services, or supplies . . . related to the health of the individual . . . [including but not limited to]: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care; *counseling*; service; or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.[95]

One question frequently asked by my students is whether a rabbi, priest, or other clergy person who provides religious or spiritual counseling or services at the hospital bedside is a health care provider, especially in the context of religious patients whose mental (and arguably physical) health depend on their faith. My students almost uniformly use their interpretive skills to answer this question in the affirmative based on the presence of the word *counseling* relative to a patient's *mental condition* in the definition of *health care* and the fact that many hospitals employ hospital chaplains and expressly list these chaplains as members of the health care team on the hospitals' websites.[96] A quick search for the word "religious" in the preamble to the Privacy Rule reveals a different interpretation by HHS, however:

93. 45 C.F.R. § 164.506(c)(1) (2016).

94. § 160.103 (italicized emphasis added) (defining health care provider).

95. *Id.* (italicized emphasis added) (defining health care).

96. *See, e.g.*, *Your Healthcare Team*, CONFLUENCE HEALTH, https://www.confluencehealth.org/patient-information/your-hospital-stay/healthcare-team/ [https://perma.cc/TFG9-UEWM] (including "chaplain" in the list of "[p]atient care team members").

> Also, in response to the comment regarding religious practitioners, the Department clarifies that "health care" as defined under the rule does not include methods of healing that are solely spiritual. Therefore, clergy or other religious practitioners that provide solely religious healing services are not health care providers within the meaning of this rule, and consequently not covered entities for the purposes of this rule.[97]

If my students had relied on their interpretations (when in practice), they would have advised their clients incorrectly, perhaps encouraging a Privacy Rule violation. I use this example to encourage my students to always check the preamble for answers before relying on their own reasonable interpretations. I also use this example to show how quickly word searches can be conducted within the preamble to yield correct answers.

A second example relates to the status of organ procurement organizations (OPOs) under the Privacy Rule. I used to represent a number of OPOs in a variety of civil, regulatory, and transactional matters. When the Privacy Rule's April 14, 2003, compliance date neared, several of my OPO clients asked me whether they were covered health care providers that were required to comply with the Privacy Rule. Given that my OPO clients evaluated and procured deceased-donor organs for transplantation, a reasonable legal interpretation of the definition of health care provider[98] might be that OPOs provide therapeutic services. In particular, they are responsible for matching organs to patients who need organs based on donor blood type, height, weight, and other medical factors, as well as proximity to the donor hospital,[99] and helping make those organs available for transplantation. However, a quick search for the phrase "organ procurement organization" within the preamble reveals a different interpretation by HHS:

> *Comment*: Some commenters suggested that blood centers and plasma donor centers that collect and distribute source plasma not be considered covered health care providers because the centers do not provide "health care services" and the blood donors are not "patients" seeking health care. Similarly, commenters expressed concern that organ procurement organizations might be considered health care providers.
>
> *Response*: We agree and have deleted from the definition of "health care" the term "procurement or banking of blood, sperm, organs, or any other tissue for administration to patients."

I use this example, again, to encourage my students to check the preamble before relying on their own Privacy Rule interpretations.

97. *See* 2000 Final Rule, *supra* note 19, at 82,568.

98. *See* text accompanying *supra* note 94 (defining health care provider).

99. *See, e.g.*, *How Organs Are Matched*, UNITED NETWORK FOR ORGAN SHARING, https://www.unos.org/transplantation/matching-organs/ [https://perma.cc/6SFW-XJ6Q] (describing the ways in which OPOs help facilitate organ transplantation).

A second source of HHS guidance is the formal guidance documents published by HHS on a wide variety of topics.[100] These guidance documents are invaluable for teaching the tricky use-and-disclosure requirements to law students. The regulation codified at 45 C.F.R. § 164.506(c)(4) nicely illustrates this point. Although the Privacy Rule allows covered entities to freely use and disclose PHI to carry out their own TPO under 45 C.F.R. § 164.506(c)(1), the Privacy Rule strictly regulates covered entities' disclosures of PHI to other individuals and institutions for the recipients' health care operations (HCO) activities under 45 C.F.R. § 164.506(c)(4). Under this regulation, a covered entity may disclose PHI for another individual's or entity's HCO without the prior authorization of the individual who is the subject of the PHI, but only if four requirements have been satisfied: (1) the recipient individual or entity also is a covered entity; (2) both the sending and receiving covered entities have had in the past or have now a relationship with the individual who is the subject of the PHI to be disclosed; (3) the PHI to be disclosed pertains to that relationship; (4) the purpose of the disclosure is listed in the first or second paragraph of the definition of HCO[101] or is a health care fraud and abuse detection or compliance activity.[102]

Ensuring student comprehension of this regulation is difficult, in part because no judicial opinion provides an example of a disclosure that is, or is not, permitted by this regulation. However, HHS has released a guidance document titled "Uses and Disclosures for Treatment, Payment, and Health Care Operations" that provides an example of a permissible disclosure: "A health care provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information."[103] When students ask me to provide a clear example of a disclosure permitted by 45 C.F.R. § 164.506(c)(4), I point them to this guidance document. After reading the

100. *See supra* note 90 (referencing the guidance documents published by HHS on a variety of Privacy Rule topics).

101. The definition of health care operations contains six long paragraphs, some of which have numerous clauses and/or sub-parts. *See* 45 C.F.R. § 164.501 (2016) (defining health care operations). The first and second paragraphs of the definition include activities relating to quality assessment and improvement, reviewing the competence or qualifications of health care professionals, licensing, certification, accreditation, training of health care professionals, and training of non-health care professionals. The third through sixth paragraph of the definition include activities such as underwriting, legal services, business planning and development, fundraising, and creating de-identified health information. *See id.*

102. 45 C.F.R. § 164.506(c)(4) (2016).

103. *Uses and Disclosures for Treatment, Payment, and Health Care Operations*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf [https://perma.cc/6CU7-C4SP] (providing this example).

guidance document, the students typically report how helpful it is, especially because it provides other examples of PHI uses and disclosures that may (or may not) be made under all the different paragraphs within 45 C.F.R. § 164.506. The students also report that this particular guidance document reads like an *Examples and Explanations* (E&E) resource,[104] which they find helpful for studying first-year and Bar subjects.

HHS's formal guidance documents are helpful in other contexts as well. The Privacy Rule's marketing provisions, for example, are quite complex, and my students frequently ask me to provide examples of communications that meet the definition of marketing and, for those that do, communications that require prior written authorization. As background, in one of the many sets of definitions within the Administrative Simplification Rules,[105] HHS defines marketing as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."[106] However, HHS excepts from the definition of marketing communications that are made:

> (i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication. (ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication: (A) For treatment of an individual by a health care provider, including 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; (B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and 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; or (C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related

104. *See Examples & Explanations*, WOLTERS KLUWER, http://www.wklegaledu.com/series/examples-explanations [https://perma.cc/P572-Z3N9] (providing information regarding the popular E&E series).

105. HHS codified definitions applicable to the Administrative Simplification Rules (Rules) in several different places throughout the Rules, including 45 C.F.R. §§ 160.103, 160.202, 160.401, 160.502, 162.103, 164.103, 164.304, 164.402, 164.501 (2016).

106. *See* 45 C.F.R. § 164.501 (2016) (defining marketing).

> functions to the extent these activities do not fall within the definition of treatment.[107]

The Privacy Rule generally requires a covered entity to obtain an authorization from an individual before using or disclosing the individual's PHI for an activity that falls within the definition of marketing. And, if the marketing activity involves financial remuneration, the Privacy Rule requires the written authorization form to identify such remuneration.[108] However, the Privacy Rule does not require a covered entity to obtain an authorization from an individual before using or disclosing the individual's PHI for marketing that takes the form of a "face-to-face communication made by a covered entity to an individual" or a "promotional gift of nominal value provided by the covered entity."[109]

Practicing health care attorneys have written volumes about the confusing nature of the Privacy Rule's marketing provisions.[110] If practicing health care attorneys struggle with the Privacy Rule's marketing provisions, it is no surprise that my law students do as well. However, HHS released a guidance document devoted to marketing that walks students through each step of the analysis; that is, (1) whether a communication meets the definition of marketing or is excepted from the definition of marketing; and (2) for those that meet the definition of marketing, whether a prior written authorization is required or whether an exception to the authorization requirement exists.[111] In addition to the straightforward two-step analysis, the guidance document also provides plenty of real-world examples of communications that do and do not fall within the definition of marketing as well as communications that do and

107. *Id.*

108. § 164.508(a)(3)(ii).

109. § 164.508(a)(3)(i).

110. *See, e.g.*, Jay Hodes, *The HIPAA Privacy Rule – What Is Often Confusing About Some of the Requirements?*, LINKEDIN (Aug. 19, 2015), https://www.linkedin.com/pulse/hipaa-privacy-rule-what-often-confusing-some-jay-hodes [https://perma.cc/83RK-TRNB] ("Another confusing area of the HIPAA Privacy Rule concerns marketing."); Gerard Clum, *HIPAA and the "Marketing" Quandary*, DYNAMIC CHIROPRACTIC (Mar. 10, 2003), http://www.dynamicchiropractic.com/pdf_out/DynamicChiropractic.com-HIPAA-and-the-Marketing-Quandary-1486844179.pdf [https://perma.cc/6PXW-5UTN] ("One of the more confusing aspects of HIPAA involves the concept of 'marketing,' and your ability to use protected health information (PHI) for marketing purposes."); Peter D. Ricoy, *Marketing Under the HIPAA Megarule: The Rule Becomes Tighter*, ABA HEALTH E-SOURCE (May 2013), http://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1305_ricoy.html [https://perma.cc/EGH6-Y4PA] ("By design, using an individual's protected health information ('PHI') for marketing purposes has never been easy under the HIPAA Privacy Rule.").

111. *Marketing*, U.S. DEP'T HEALTH & HUMAN SERVS., 1, 1–4 (Apr. 3, 2003), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf [https://perma.cc/4GFU-97CY].

do not require prior written authorization.[112] My students have reported success in using HHS's guidance on marketing to learn the Privacy Rule's marketing provisions.

In addition to the preamble language and the formal guidance documents, another source of helpful teaching material includes HHS's answers to the hundreds of publicly-submitted, frequently-asked questions regarding the Privacy Rule.[113] One question my students frequently ask me is whether contracted researchers who conduct research on behalf of a covered entity fall within the definition of a business associate of the covered entity due to the performance of such research. The question is a good one because the Privacy Rule defines a *business associate* to include persons who, with respect to a covered entity but other than in the capacity of a workforce member of the covered entity, "creates, receives, maintains, or transmits protected health information for a function or activity *regulated* by . . . [the Privacy Rule]").[114] The Privacy Rule heavily regulates research at 45 C.F.R. § 164.512(i).[115] A reasonable, logical interpretation of the definition of business associate, then, is that a contracted researcher who creates PHI while conducting research for the covered entity is a business associate of the covered entity. However, HHS's answer to frequently-asked question number 239 provides a different interpretation:

> *Question*: Is a business associate contract required for a covered entity to disclose protected health information to a researcher?
>
> *Answer*: No. Disclosures from a covered entity to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103.[116]

A final, illustrative source of outstanding teaching material includes the resolution agreements. HHS has entered into dozens of resolution agreements with covered entities pursuant to which a covered entity accused by HHS of violating the Privacy Rule agrees to perform certain obligations and make

112. *Id.* at 2–4.

113. *HIPAA FAQs for Professionals*, *supra* note 91.

114. 45 C.F.R. § 160.103 (2016) (emphasis added) (defining "business associate").

115. § 164.512(i) (regulating "[u]ses and disclosures for research purposes").

116. *Is a Business Associate Contract Required for a Covered Entity to Disclose Protected Health Information to a Researcher?*, U.S. DEP'T HEALTH & HUMAN SERVS. (Dec. 19, 2002), http://www.hhs.gov/hipaa/for-professionals/faq/239/is-a-business-associate-contract-required-for-a-covered-entity-to-information-to-a-researcher/index.html [https://perma.cc/GWD2-2ACD].

reports to HHS, generally for a period of three years, and to pay a fine to HHS. These resolution agreements can be very instructive in terms of teaching questions that are not specifically answered by the Privacy Rule.

One question that I frequently encountered in my practice—and about which many students have asked over the years as well—is the question whether a covered hospital is permitted to allow a film crew to film patients in the emergency room in order to produce a reality television show that can generate extra revenue for the hospital. Importantly, the camera men would obtain the authorization of all filmed patients prior to releasing the final television video to a network. As a conservative attorney, I always answered my clients and my students in the negative based on my gut, which told me that HHS would view this as an unauthorized disclosure of PHI (including the patients' faces and their emergent physical conditions) by the hospital to the cameramen, although any subsequent disclosure of the film by the cameramen to a television network certainly would be authorized. However, many of my less conservative colleagues disagreed. Until recently, neither the Privacy Rule nor any HHS guidance provided clear answers.

On April 19, 2016, however, OCR entered into a resolution agreement ("Agreement") with New York Presbyterian Hospital ("Hospital") following the Hospital's unauthorized disclosure of two patients' PHI to an ABC television film crew ("ABC"). As background, the Hospital allowed ABC to film one patient's death and a second patient's significant clinical distress without the patients' or their legal representatives' prior written authorization in violation of the default rule summarized in Part II of this Article[117] in order to produce the "high stakes medicine" reality television show, *NY Med*.[118] In its press release announcing the Agreement, OCR stated, "[The Hospital's] actions blatantly violate the HIPAA Rules, which were specifically designed to prohibit the disclosure of individual's PHI, including images, in circumstances such as these."[119] OCR further stated that the Hospital "failed to safeguard protected health information and allowed ABC film crews virtually unfettered access to its health care facility, effectively creating an environment where PHI could not be protected from impermissible disclosure to the ABC film crew and staff."[120] In addition to agreeing to pay OCR $2.2 million, the Hospital also executed a corrective action plan pursuant to which the Hospital agreed to

117. *See* text accompanying *supra* notes 63–65 for a summary of the default rule.

118. *About NY Med*, ABC, http://abc.go.com/shows/ny-med/about-the-show [https://perma.cc/R9AE-4CKJ] ("Sometimes poignant and often uproarious, [NY Med] takes a deep dive into high stakes medicine through the eyes of unforgettable characters . . . . ").

119. *Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital*, U.S. DEP'T HEALTH & HUMAN SERVS. (Apr. 21, 2016), http://www.hhs.gov/about/news/2016/04/21/unauthorized-filming-ny-med-results-22-million-settlement-new-york-presbyterian-hospital.html [https://perma.cc/KJ6G-P8UZ].

120. *Id.*

monitoring by OCR for a period of two years.[121] I assigned this resolution agreement as reading in my Spring 2017 HIPAA Privacy class.

C. Teaching Non-Law Audiences

Parts III (A) and (B), above, discussed methods of teaching the Privacy Rule to law students. I am frequently asked to teach physicians, dentists, clinical psychologists, social workers, nurses, and other non-law professionals, including Privacy officials and compliance officers, regarding their obligations under the Privacy Rule. These presentations usually are one or two hours in length and the attendees usually receive continuing ethics education ("CE") credit for attending. When I first started providing CEs on the Privacy Rule to non-law-trained professionals, I would borrow PowerPoints I had created for my law students. These PowerPoints typically included much background regarding the Privacy Rule, including references to all the different proposed, interim final, and final rulemakings. Being the detailed lawyer that I am, I would carefully review the administrative history that led to the regulations that are now codified at 45 C.F.R. § 164 and provide a bird's-eye legal overview of the different provisions in the HIPAA and HITECH statutes as well as the Privacy Rule, including not only the use-and-disclosure requirements, but also the individual rights, the breach notification requirements, and the administrative requirements. During the short question-and-answer session after each presentation, I could tell by the questions that the health care professionals were either uninterested in, or simply unable to digest, my heavy-in-administrative-law lecture.

After one presentation that was particularly poorly received, I asked a neurology residency program director who attended how I could improve going forward. The residency program director said he had an idea; that is, he would ask his residents to submit all their Privacy Rule questions to me in advance. Then, I could devote my presentation time to the questions in which they were interested, rather than the administrative topics in which I was interested. We followed this plan shortly thereafter.

When I received the questions from the residency program director, I realized they all focused on the Privacy Rule's use-and-disclosure requirements. I also realized that the questions focused almost exclusively on the question whether PHI could be used or disclosed in a particular situation with or without prior patient authorization. None of the questions related to the

121. New York Presbyterian Hospital Resolution Agreement, *supra* note 37, at 2, § 6 ("HHS has agreed to accept, and NYP has agreed to pay HHS, the amount of $2,200,000 . . . . "); *id.* at § 7 ("[The Hospital] has entered into and agrees to comply with the Corrective Action Plan ('CAP') . . . . If [the Hospital] breaches the CAP, and fails to cure the breach as set forth in the CAP, then [the Hospital] will be in breach of this Agreement and HHS will not be subject to the Release . . . . ").

administrative history of the Privacy Rule, the personnel designations required by the Privacy Rule, the policies and procedures required by the Privacy Rule, the compliance dates for the Privacy Rule, or the possible civil and criminal penalties for violations of the Privacy Rule.

I organized the questions I received in order of the use and disclosure requirements codified at 45 C.F.R. §§ 164.502–514, with the TPO questions early in the presentation and the public benefit disclosures later in the presentation. Then, I opened my presentation by reviewing the three use-and-disclosure rules summarized in Part II of this Article. Finally, I answered each question using one of those three rules. By the end of the CE program, the physicians who attended understood the three-tiered approach to individual permission and were able to answer their own Privacy Rule questions with reference to the regulations codified at 45 C.F.R. §§164.502–514.

CONCLUSION

This Article has summarized the history of the Privacy Rule, reviewed the Privacy Rule's theory of and approach to health information confidentiality, and discussed my experience teaching the Privacy Rule to both law and non-law audiences. In part because few judicial opinions interpreting the Privacy Rule are substantively helpful, this Article suggests that Privacy Rule teachers may wish to teach fewer cases and focus instead on the principles of health information confidentiality gleaned from the preambles to HHS's rulemakings as well as HHS's guidance documents, resolution agreements, and frequently asked questions. This Article also suggests that Privacy Rule teachers who train non-law audiences solicit questions in advance and use these questions to illustrate the Privacy Rule's use-and-disclosure requirements, as bird's-eye legal overviews tend to be unhelpful.