2016

Complying with the HIPAA Privacy Rule: Problems and Perspectives

Stacey A. Tovino
University of Nevada, Las Vegas -- William S. Boyd School of Law

Complying with the HIPAA Privacy Rule: Problems and Perspectives

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

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 a final rule governing the use and disclosure of protected health information by covered entities and their business associates (Privacy Rule).[5]

This Article addresses the question of what it means for covered entities and business associates to comply with the Privacy Rule. In particular, this Article will examine the challenges covered entities and business associates face in attempting to comply with the Privacy Rule while delivering and supporting the delivery of health care in an administratively responsible and financially feasible manner.

---

*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) and Andrew Martineau (Research Librarian, Wiener-Rogers Law Library) for locating many of the sources referenced herein.

1. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in various sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.) [hereinafter HIPAA].

2. *See infra* notes 19–34 (referencing several sets of proposed, interim final, and final rules).

3. HIPAA, *supra* note 1, at Title II, Subtitle F, §§ 261–264 [hereinafter Administrative Simplification Provisions].

4. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, §§ 13001–13424 (Feb. 17, 2009) [hereinafter ARRA] (containing the Health Information Technology for Economic and Clinical Health (HITECH) Act).

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

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 identifies three themes relating to Privacy Rule compliance.[8]

First, some Privacy Rule provisions are simply too complex to be operationalized.[9] Covered entities and business associates with the financial means to do so can hire outside counsel to draft sophisticated policies and procedures and conduct HIPAA-compliant training sessions for workforce members, but many regulated actors are unable to fully operationalize all of the Privacy Rule's requirements due to the Rule's complexity and the costs associated with compliance.[10]

Second, some covered entities continue to value revenue generation over Privacy Rule compliance.[11] Financially struggling non-profit hospitals and other health industry participants can generate revenue by selling protected healthcare information (PHI) to marketing companies, using and disclosing PHI for fundraising activities, and entering into side businesses, including reality television show production.[12] The Privacy Rule prohibits most of these information uses and disclosures unless the covered entity obtains prior written authorization from the individuals who are the subject of the information being used and disclosed. However, research reveals that some covered entities do not obtain authorization before engaging in these lucrative activities.

Third, mobile technology and portable records continue to challenge privacy rule compliance.[13] Although laptop computers, tablets, thumb drives, and smart phones are necessary for the modern practice of medicine, these technologies can increase the risk of health information confidentiality breaches if not used carefully. Research reveals several cases in which employees and independent contractors of covered entities have negligently failed to secure such technology, resulting in significant health information confidentiality breaches.

---

6. *See infra* Part I.
7. *See infra* Part II.
8. *See infra* Part III.
9. *See infra* Part III(A).
10. *See id.*
11. *See infra* Part III(B).
12. *See id.*
13. *See infra* Part III(C).

I. HISTORY OF THE PRIVACY RULE

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.[14] The Administrative Simplification Provisions[15] directed HHS to issue regulations protecting the privacy[16] of individually identifiable health information if Congress failed to enact comprehensive privacy legislation within three years of HIPAA's enactment.[17] When Congress failed to enact privacy legislation by its deadline, HHS incurred the duty to adopt privacy regulations.[18] 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

14. *See* HIPAA, *supra* note 1, at Preface ("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." *Id.*)

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

16. 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 Magnetic Resonance Information: A Case for Neuro Exceptionalism?* 34 FLA. ST. U.L. REV. 415, 441–470 (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.* Confidentiality, on the other hand, refers to the obligation of a health industry participant to 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*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Aug. 9, 2016).

17. Administrative Simplification Provisions, *supra* note 3, § 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…." *Id.*)

18. *See id.*

entities).[19]

HHS responded. On November 3, 1999,[20] and December 28, 2000,[21] HHS issued a proposed and final privacy rule (Privacy Rule) regulating covered entities' uses and disclosures of PHI. On March 27, 2002,[22] and August 14, 2002,[23] HHS issued proposed and final modifications to the Privacy Rule. With the exception of technical corrections and conforming amendments,[24] 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)[25] changed significantly more than seven years ago. On February 17, 2009, President Obama signed ARRA into law.[26] 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

---

19. *Id.* § 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; Proposed Rule, 64 Fed. Reg. 59,918, 59,924 (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).

20. *Id.* at 59,918.

21. Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000) [hereinafter 2000 Final Rule].

22. Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 67 Fed. Reg. 14,776 (Mar. 27, 2002).

23. Standards for Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53,182 (Aug. 14, 2002).

24. *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, Final Rule; Correction of Effective and Compliance Dates, 66 Fed. Reg. 12,434 (Feb. 26, 2001); Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000, 65 Fed. Reg. 82,944 (Dec. 29, 2000) [hereinafter Technical Corrections I].

25. 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. 5,566, 5,688 (Jan. 25, 2013) [hereinafter Final Regulations] (adopting 45 C.F.R. § 160.103 and providing a new definition of business associate).

26. ARRA, *supra* note 4.

violate the Privacy Rule.[27]

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.[28] On October 30, 2009, HHS released an interim final rule implementing HITECH's strengthened enforcement provisions, including strengthened civil monetary penalties that the federal 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.[29] On May 31, 2011, HHS released a proposed rule that would modify the HIPAA Privacy Rule's accounting of disclosures requirement.[30] 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).[31] On June 7, 2013, HHS released technical corrections to the Final Regulations.[32] On September 16, 2013, HHS released a Model Notice of Privacy Practices designed to assist covered entities in complying with the Final Regulations.[33] 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.[34] Most recently, on January 6, 2016, HHS released

---

27. HITECH, *supra* note 4. 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, 813-867 (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 works by demonstrating the difficulty many covered entities and business associates have with Privacy Rule compliance.

28. Breach Notification for Unsecured Protected Health Information, Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

29. HIPAA Administrative Simplification: Enforcement, Interim Final Rule, 74 Fed. Reg. 56,123 (Oct. 30, 2009).

30. Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act, Proposed Rule, 76 Fed. Reg. 31,426 (May 31, 2011).

31. *See* Final Regulations, *supra* note 25.

32. *See* Technical Corrections to the HIPAA Privacy, Security, and Enforcement Rules, Final Rule, 78 Fed. Reg. 32466, 32466 (June 7, 2013) [hereinafter Technical Corrections II].

33. *Model Notices of Privacy Practices*, HHS.GOV http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/ (last visited Aug. 11, 2016) [hereinafter Model Notice].

34. CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports; Final

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 the identities of individuals who are disqualified from shipping, transporting, possessing, or receiving a firearm.[35]

As of this writing, HHS also has released thirty-nine 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 amount.[36] A recent resolution agreement, executed by HHS and New York Presbyterian Hospital (Hospital) on April 19, 2016, required the Hospital to pay HHS $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 proceeding. The Privacy Rule has as its goal the balancing of 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

---

Rule, 79 Fed. Reg. 7290 (Feb. 6, 2014).

35. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS) and the National Instant Criminal Background Check, Final Rule, 81 Fed. Reg. 382 (Jan. 6, 2016).

36. *See Resolution Agreements: Resolution Agreements and Civil Money Penalties*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last visited Sept. 5, 2016).

37. *See Resolution Agreement and Corrective Action Plan Between HHS and New York and Presbyterian Hospital* HHS.GOV (Apr. 19, 2016), http://www.hhs.gov/sites/default/files/nyp-nymed-racap-april-2016.pdf [hereinafter New York Presbyterian Hospital Resolution Agreement].

38. *See* 2000 Final Rule, *supra* note 21, 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 IIHI as "information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or

not constitute (1) an education record protected under the Family Educational Rights and Privacy Act of 1974 (FERPA);[40] (2) a student treatment record excepted from protection under FERPA;[41] (3) an employment record held by a covered entity in its role as an employer;[42] or (4) individually identifiable health information regarding a person who has been deceased for more than 50 years.[43] The name given by the Privacy Rule to the subset of IIHI described in the previous sentence is protected health information (PHI).[44]

Before using or disclosing PHI, the Privacy Rule requires covered entities and BAs to adhere to one of three different rules depending on the purpose of the information use or disclosure.[45] 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.[46]

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

---

received by a health care provider, 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." *See* 45 C.F.R. § 160.103 (2016).

40. *Id.* § 160.103 (defining protected health information).

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.* (using the phrase protected health information).

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

46. *See* text accompanying *supra* note 39.

treatment,[47] payment,[48] and health care operations[49] activities,[50] as well as certain public benefit activities.[51]

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.[52] 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.[53] 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.[54] 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.[55] By final illustrative example, a covered entity may disclose

47. The Privacy Rule defines 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." 45 C.F.R. § 164.501 (2016).

48. 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.* § 164.501.

49. The Privacy Rule defines health care operations with respect to a list of activities that are related to a covered entity's covered functions. *See 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.*

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

51. 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. *See id.* § 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 id.* § 164.512(a), (c), (f), (i), and (l).

52. *See id.* § 164.501 ("Treatment means. . .consultation[s] between health care providers relating to a patient").

53. *See id.* ("Payment means. . .[t]he activities undertaken by. . .[a] health care provider. . .to obtain. . .reimbursement for the provision of health care.") (permitting a covered entity to disclose PHI for its own payment activities).

54. *See id.* ("Health care operations means. . .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.").

55. *See id.* § 164.512(a) ("A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure

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.[56] The theory behind these permitted information uses and disclosures is that treating patients, allowing health care providers to obtain 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.[57] 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.[58] 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;[59] (2) certain uses and disclosures that would allow other persons to be involved in a patient's care or payment for care;[60] (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;[61] (4) certain uses and disclosures for disaster relief purposes;[62] 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.[63]

---

is limited to the relevant requirements of such law.").

56. *See id.* § 164.512(f)(4).
57. *See id.* § 164.510.
58. *See id.*
59. *See id.* § 164.510(a).
60. *See id.* § 164.510(b)(1)(i).
61. *See id.* § 164.510(b)(1)(ii).
62. *See id.* § 164.510(b)(4).
63. *See id.* § 164.510(b)(5).

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.[64] Likewise, a woman in labor who wishes her partner to be present for her labor and delivery may orally give her permission for her health care providers to involve her partner in her care.[65]

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.[66]

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.[67] 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

64. *See id.* § 164.510(a)(1), (2).
65. *See id.* § 164.510(b)(1)(i).
66. *See id.* § 164.508(a)(1).
67. *See id.* § 164.508(c)(1) and (2).

marketing company to allow the company to market its products and services to the individual.[68]

With this background regarding the Privacy Rule's theory and approach to health information confidentiality, Part III of this Article will examine three challenges associated with Privacy Rule compliance.

III. PROBLEMS AND PERSPECTIVES

A. Some Privacy Rule Provisions Are Too Complex to be Operationalized

A principal problem with the Privacy Rule is its complexity, especially with respect to the regulatory provisions governing (1) disclosures of PHI from one covered entity to another covered entity for the recipient covered entity's health care operations activities;[69] (2) uses and disclosures of PHI for marketing;[70] and (3) uses and disclosures of PHI for public benefit activities.[71] One result is that covered entities frequently hire outside counsel to write HIPAA-compliant policies and procedures, especially with respect to the more complex Privacy Rule provisions identified above. I served as outside counsel to many of the covered entities located in Houston's Texas Medical Center from the mid-1990s through the mid-2000s, and I drafted for those covered entities many of the policies and procedures required by the Privacy Rule.[72] To make the policies and procedures HIPAA-compliant,[73] I had to include references to the Privacy Rule's complex provisions. Regardless of the number of times that I explained the provisions to my clients and regardless of the number of live trainings that I provided to my clients' administrators, medical staff members, nursing staff members, and other workforce members, the provisions were simply too difficult to be operationalized. Thus, my clients were able to demonstrate what I call "paper," but not true, compliance with the Privacy Rule. Allow me to provide a few examples of this problem.

---

68. *See* 2000 Final Rule, *supra* note 21, at 82,514 ("[C]overed entities must obtain the individual's authorization before using or disclosing protected health information for marketing purposes.").

69. 45 C.F.R. § 164.506(c)(4) (2016).

70. *See id.* § 164.501 (defining marketing); *id*. § 164.508(a)(3) (regulating the use and disclosure of PHI for marketing).

71. *See id.* § 164.512(a)-(l).

72. *See id.* § 164.530(i)(1) ("A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of [the Privacy Rule]. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance.").

73. *See id.*

1. HCO Disclosures

As discussed in Part II, the Privacy Rule requires covered entities to comply with one of three rules before using or disclosing PHI.[74] The first rule 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.[75] The regulation that allows these uses and disclosures[76] is frequently referred to as the TPO rule.

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),[77] 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).[78] 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 five 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[79] or is a health care fraud and abuse detection or compliance activity; and (5) the PHI disclosed is limited to the PHI that is minimally necessary to accomplish the intended purpose of the disclosure.[80] Most covered entities have a complex policy and procedure, usually drafted by outside counsel, identifying when the covered entity may disclose PHI to another entity for that entity's HCO under the Privacy Rule.[81]

---

74. *See* text accompanying notes 45–68 .

75. 45 C.F.R. § 164.506(c)(1) (2016).

76. *See id.*

77. *See id.*

78. *See id.* § 164.506(c)(4).

79. The definition of health care operations contains six long paragraphs, some of which have numerous clauses and/or sub-parts. *See id.* § 164.501 (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. *See id.* 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.*

80. *See id.* § 164.506(c)(4).

81. *See, e.g.*, *Privacy Policies & Procedures: Section 3—Uses and Disclosures to Carry out Treatment, Payment, or Health Care Operations*, OKLA. ST. UNIV. CTR. FOR HEALTH SCI. (rev. July 1, 2013), https://centernet.okstate.edu/hipaa/privacyprocedures3.php#0301

Even with a written policy and procedure available to provide guidance, compliance by a covered entity with the regulation described in the previous paragraph is difficult. That is, the regulation requires the sending covered entity to (1) make a legal determination whether the receiving entity is a covered entity when many non-lawyer administrators, physicians, nurses, and other business and health care professionals are not trained regarding how to determine which individuals and institutions meet the definition of a covered entity under the Privacy Rule;[82] (2) trust the receiving entity when it states that it has had or has now a relationship with the individual whose PHI is being requested; (3) determine whether the PHI being requested pertains to that relationship; (4) trust the receiving entity when it states that the reason it wants the PHI is for an activity that falls within the first or second paragraph of the definition of health care operations or constitutes a health care fraud and abuse detection or activity or, if the receiving entity is not familiar with the definition of health care operations, make its own legal determination regarding whether the receiving entity's proffered reason for wanting the PHI falls within the first or second paragraph of the definition of health care operations or constitutes a health care fraud and abuse detection and compliance activity; and (5) make a determination whether the PHI requested is the minimal amount of PHI necessary to accomplish the requestors HCO.

One might argue that a non-lawyer workforce member of a covered entity who is faced with a request for a disclosure of PHI for the receiving entity's HCO could simply ask the covered entity's general counsel whether the disclosure is permitted by 45 C.F.R. § 164.506(c)(4). However, large hospitals and other large covered entities are asked to disclose PHI for the HCO of other entities hundreds of times each week. Calling general counsel and waiting for counsel to respond every single time a request for PHI is made is simply not feasible. Further, many covered entities do not have general counsel and calling outside counsel several times a day or week is not financially feasible.

One result is that many covered entities simply ignore the Privacy Rule and either allow all, or refuse all, requests for disclosures of PHI for the requesting entity's HCO. That is, many covered entities are unable to operationalize the Privacy Rule's complex provisions and instead (1) always disclose requested information without regard to the Privacy Rule, thus possibly violating the Privacy Rule; or (2) always refuse to disclose requested information, even when the Privacy Rule would have permitted the disclosure due to the societal value of the disclosure.

(addressing disclosures for HCO); *Privacy and Security Policies of BSHC*, BOS. SENIOR HOME CARE 1, 10, https://bostonseniorhomecare.info/download/BSHC_full_Privacy_Policies.pdf (last visited Aug. 11, 2016) (same).

82. *See* text accompanying *supra* note 19 (defining covered entities).

2. Marketing Uses and Disclosures

Allow me to provide a second example of a Privacy Rule provision that is too complex to be operationalized. In one of the many sets of definitions within the Administrative Simplification Rules,[83] 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."[84] However, HHS excepts from the definition of marketing communications that are made:

> (1) 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; (2) 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 functions to the extent these activities do not fall within the definition of treatment.[85]

The Privacy Rule generally requires a covered entity to obtain an

---

83. 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, and 164.501 (2016).

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

85. *Id*. § 164.501.

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.[86] 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."[87]

Practicing health care attorneys have written volumes about the confusing nature of the Privacy Rule's marketing provisions.[88] In these writings, lawyers attempt to explain to business and health care professionals which communications meet the definition of marketing,[89] which communications are excepted from the definition of marketing,[90] and which communications meet the definition of marketing but are otherwise excepted from the authorization requirement.[91] During my decade of practice, I received hundreds of requests from hospital administrators, health care providers, and even general counsel asking for clarification regarding these questions. Many times, my general counsel clients would ask me, "If I cannot understand these provisions and I am in-house counsel, how can I expect my workforce members to implement them?"

In response, I would draft a HIPAA-compliant marketing policy so my client would, at the very least, be able to demonstrate paper compliance with the policies and procedures requirement set forth in the Privacy Rule[92] should the client be audited by OCR.[93] But having a HIPAA-compliant policy on

86. *Id*. § 164.508(a)(3)(ii).

87. *Id*. § 164.508(a)(3)(i).

88. *See, e.g.*, Jay Hodes, *The HIPAA Privacy Rule—What is Often Confusing About Some of the Requirements?*, LINKEDIN PULSE (Aug. 19, 2015), https://www.linkedin.com/pulse/hipaa-privacy-rule-what-often-confusing-some-jay-hodes ("Another confusing area of the HIPAA Privacy Rule concerns marketing."); Gerard Clum, *HIPAA and the "Marketing" Quandary*, 21 DYNAMIC CHIROPRACTOR (Mar. 10, 2003), http://www.dynamicchiropractic.com/mpacms/dc/article.php?id=9069 ("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*, 9 A.B.A. HEALTH E-SOURCE (2013), http://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1305_ricoy.html ("By design, using an individual's protected health information ('PHI') for marketing purposes has never been easy under the HIPAA Privacy Rule.").

89. *See* text accompanying *supra* note 88.

90. *See* text accompanying *supra* note 88.

91. *See* text accompanying *supra* note 88.

92. *See* text accompanying *supra* note 72.

93. *See HIPAA Privacy, Security, and Breach Notification Audit Program*, HHS.GOV,

paper is not the same thing as having an educated workforce that understands, implements, and/or adheres to the policy. I learned this lesson the hard way; that is, when a client for whom I had drafted a HIPAA-compliant marketing policy later revealed that he had not obtained prior written authorization from patients to whom he was clearly sending marketing communications because he still could not figure out what was—and was not—a marketing communication.

3. Law Enforcement Disclosures

A third example of a Privacy Rule provision that is too complex to be operationalized as quickly as it needs to be governs law enforcement requests for PHI. As discussed in Part II, covered entities may use and disclose PHI for twelve public benefit activities without obtaining the prior written authorization of the individuals whose PHI is being used or disclosed.[94] Most of these public benefit activities contain numerous conditions, requirements, or criteria that must be satisfied before the Privacy Rule waives prior written authorization.

For example, the sixth public benefit exception relates to disclosures of PHI to law enforcement officers for law enforcement purposes.[95] This exception identifies six sub-situations when a covered entity is permitted to disclose PHI to a law enforcement official for a law enforcement purpose without prior written authorization, with each sub-situation containing detailed conditions precedent to the disclosure.[96] One of the six sub-situations involves victims of a crime.[97] This particular provision permits a covered entity to disclose PHI without prior written authorization, but only if (1) the recipient is a law enforcement official, defined as an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to (A) investigate or conduct an official inquiry into a potential violation of law; or (B) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law;[98] and (2) a law enforcement official affirmatively requests the information (and the covered entity is not initiating a voluntary disclosure of PHI to the law

---

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/ (last visited June 21, 2016) ("The 2016 Phase 2 HIPAA Audit Program will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the [Privacy Rule and other Administrative Simplification Rules].").

94. *See* 45 C.F.R. § 164.512(a)-(l) (2016); text accompanying *supra* note 52.
95. *See* 45 C.F.R. § 164.512(f) (2016).
96. *See id.* § 164.512(f)(1)–(6).
97. *See id.* § 164.512(f)(3).
98. *See id.* § 164.103 (defining law enforcement official).

enforcement official); and (3) the law enforcement official is requesting information about an individual who is or is suspected to be a victim of a crime (when some covered entity workforce members have no training in determining when to suspect an individual is a victim of a crime); and (4) the individual who is the subject of the requested PHI agrees to the disclosure; or (5) the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, and (A) the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; (B) the law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (C) the disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.[99]

Although general counsel or outside counsel certainly could assist a covered entity's workforce member in making a determination whether a disclosure relating to a victim or suspected victim of crime would be allowed under this provision, the catch is that law enforcement officials (and other individuals, such as bounty hunters, who claim authority under state law but may or may not have actual authority depending on state law) simply show up at hospitals, many times in the emergency room, demanding PHI. Sometimes, a workforce member will fear that if he or she asks the alleged law enforcement official to wait while the workforce member consults with counsel, the workforce member will be accused of obstructing justice. Other times, a workforce member will fear if he or she discloses the PHI immediately upon request that he or she will violate the Privacy Rule, incur significant civil and criminal penalties, and/or jeopardize his or her employment as a result of violating patient confidentiality.

As with the marketing provisions discussed in Part III(A)(2), I have drafted many HIPAA-compliant paper policies designed to assist covered entities in responding to law enforcement requests for PHI. Again, having a HIPAA-compliant policy on paper is not the same thing as having an educated workforce that is capable of understanding, implementing, and/or adhering to the policy. I also learned this lesson the hard way; that is, when a client for whom I had drafted a HIPAA-compliant policy governing disclosures to law enforcement later revealed that he had disclosed PHI to both legitimate law enforcement officials as well as private investigators who did not meet the definition of a law enforcement official because he simply did not have time to figure out whether the Privacy Rule would permit the

99. *Id.* § 164.512(f)(3).

disclosure or not in the time frame in which the official or investigator was demanding the PHI.

B. Some Covered Entities Still Value Revenue Generation over Privacy Rule Compliance

The above section summarized three Privacy Rule provisions that are difficult for covered entities to operationalize due to their complexity. This section identifies a second problem with the Privacy Rule, which is that some covered entities intentionally overlook or perhaps unintentionally ignore simple Privacy Rule prohibitions when the prohibited information use or disclosure could generate revenue for the covered entity. Allow me to use the most recent Privacy Rule resolution agreement as an example.

On April 19, 2016, 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[100] in order to produce the "high stakes medicine" reality television show, NY Med.[101] 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."[102] 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."[103] 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 monitoring by OCR for a period of two years.[104]

---

100. *See* text accompanying *supra* notes 66–68 for a summary of the default rule.

101. *See NY Med*, ABC, http://abc.go.com/shows/ny-med (last visited Aug. 11, 2016) ("Sometimes poignant and often uproarious, [NY Med] takes a deep dive into high stakes medicine through the eyes of unforgettable characters. . .").

102. Press Release, U.S. Dep't of Health & Human Servs. Press Office, Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital (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.

103. *Id*.

104. New York Presbyterian Hospital Resolution Agreement, *supra* note 38, at 2, ("HHS has agreed to accept, and NYP has agreed to pay HHS, the amount of $2,200,000…."); *id*. § 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

One might be inclined to say that the Hospital simply did not understand the Privacy Rule's prohibitions and therefore did not know that it was not permitted to film patients without their authorization. However, unlike the complex Privacy Rule provisions discussed at Part III(A)(1)-(3), the Hospital violated the default rule, the simplest provision in the entire Privacy Rule. In Part II, I explained that covered entities may not use or disclose PHI without prior written authorization in any situation in which the information use or disclosure is not otherwise permitted or required by the Privacy Rule.[105] Filming one dying patient and a second clinically distressed patient—both without prior written authorization—clearly does not constitute TPO, a public benefit activity, or any other permitted or required information use or disclosure. Notwithstanding its own notice of privacy practices, which clearly states that the Hospital is "required by law to maintain the privacy and security of your protected health information,"[106] the Hospital breached two patients' privacy in order to produce a reality television show that would generate revenue.

C. Mobile Devices and Portable Records Continue to Challenge Privacy Rule Compliance

HHS adopted the Privacy Rule in part due to the growing use of electronic technology, including the shift from paper to electronic medical records and the associated increase in privacy-related risks.[107] A review of the thirty-five resolution agreements and/or civil monetary penalty (CMP) agreements into which HHS has entered suggests that basic mobile technology and portable records issues, including loss and theft of laptops and thumb drives as well as printed paper records, continue to challenge Privacy Rule compliance.

In March of 2016, for example, HHS entered into a $3.9 million resolution agreement with Feinstein Institute for Medical Research (Feinstein), a New York not-for-profit corporation sponsored by Northwell Health, Inc., a large health system including twenty-one hospitals and more than 450 patient facilities and physician practices.[108] The settlement followed a Feinstein employee's negligent decision to leave an unsecured laptop containing the PHI of 13,000 patients and research participants, including names, dates of

---

CAP, then [the Hospital] will be in breach of this Agreement and HHS will not be subject to the Release. . .").

105. *See* text accompanying *supra* notes 66–68.

106. *See Privacy Notice*, N.Y.-PRESBYTERIAN, http://www.nyp.org/pdf/privacy_notice_english.pdf (last visited Aug. 11, 2016).

107. *See* 1999 Proposed Rule, *supra* note 19, at 59,920.

108. *Resolution Agreement Between HHS & Feinstein Institute for Medical Research*, HHS.GOV, 1, 2 (Mar. 16, 2016), http://www.hhs.gov/sites/default/files/fimr-resolution-agreement-and-corrective-action-plan.pdf ("HHS has agreed to accept, and [Feinstein] has agreed to pay HHS, the amount of $3,900,000.00. . .").

birth, addresses, social security numbers, diagnoses, laboratory results, medications, and medical information, in the back seat of the employee's car.[109] The laptop was later stolen from the employee's car.[110] This resolution agreement illustrates how all of the written policies, procedures, and trainings in the world cannot protect the confidentiality of PHI if workforce members do not comply with such policies, procedures, and/or trainings. This agreement also demonstrates how Feinstein could have prevented or mitigated a breach of confidentiality by (1) conducting a risk analysis of the potential risks and vulnerabilities to the confidentiality of the PHI stored on the stolen laptop and other mobile devices; (2) implementing physical safeguards for laptops and other mobile devices containing PHI that would restrict access by unauthorized users; and (3) encrypting PHI contained on laptops and other mobile devices.[111]

Other resolution agreements and civil monetary penalty agreements reveal similar themes. On March 1, 2016, for example, OCR issued a notice of final determination imposing a $239,800 civil monetary penalty on Lincare, Inc., a provider of respiratory care, infusion therapy, and medical equipment to at-home patients (Lincare), after a Lincare employee left behind documents containing the PHI of 278 patients.[112] Similarly, on December 26, 2013, OCR announced[113] that Adult & Pediatric Dermatology, P.C., of Concord, Mass. (APDerm) entered into a $150,000 resolution agreement after an APDerm staff member left an unencrypted thumb drive containing the PHI of approximately 2,200 patients in his car.[114] The thumb drive was later stolen from the staff member's car.[115]

On September 17, 2012, by further example, HHS released a press

109. *Id*. at 1, § I(2).

110. *Id*.

111. *Id.* at 1–2, § I(2)(ii)-(vi).

112. Letter from Jocelyn Samuels, Dir., Office for Civil Rights to Mr. Marshall S. Ney, Esq., Friday, Eldredge & Clark, LLP (Mar. 1, 2016) http://www.hhs.gov/sites/default/files/lincare-nfd-for-web.pdf; Press Release, U.S. Dep't of Health & Human Servs. Press Office, Administrative Law Judge Rules in Favor of OCR Enforcement, Requiring Lincare, Inc. to Pay $239,800 (Feb. 3, 2016), http://www.hhs.gov/about/news/2016/02/03/administrative-law-judge-rules-favor-ocr-enforcement-requiring-lincare-inc-pay-penalties.html.

113. *See, e.g.*, Press Release, U.S. Dep't of Health & Human Servs. Press Office, Dermatology Practice Settles Potential HIPAA Violations (Dec. 26, 2013) http://www.hhs.gov/about/news/2013/12/26/dermatology-practice-settles-potential-hipaa-violations.html.

114. *See Resolution Agreement Between HHS and Adult & Pediatric Dermatology, P.C.*, HHS.GOV, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/apderm-resolution-agreement.pdf (last visited Aug. 11, 2016).

115. *Id*.

release[116] announcing that the Massachusetts Eye and Ear Infirmary (MEEI) entered into a $1.5 million resolution agreement following the theft of an unencrypted personal laptop containing the PHI of MEEI patients and research subjects, including patient prescriptions and clinical information.[117] Likewise, on February 24, 2011, Massachusetts General Hospital entered into a $1 million resolution agreement after an employee accidentally left documents containing the PHI of 192 infectious disease patients, including some individuals diagnosed with HIV, on the subway while commuting to work.[118]

In summary, mobile devices and portable records continue to challenge Privacy Rule compliance. Workforce members are only human and occasionally a workforce member will drop or leave behind a device or record that contains PHI. Covered entities need to anticipate these accidental behaviors by: (1) conducting risk analyses associated with mobile devices and portable records; (2) implementing physical safeguards for laptops and other mobile devices and portable records containing PHI that would restrict access by unauthorized users; and (3) encrypt PHI contained on laptops and other mobile devices.[119]

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 identified three themes relating to Privacy Rule compliance.

First, some Privacy Rule provisions are too complex to be operationalized. Covered entities with the financial means to do so can hire outside counsel

---

116. *See* Press Release, U.S. Dep't of Health & Human Servs. Press Office, Massachusetts Provider Settles HIPAA Case for $1.5 Million (Sept. 17, 2012), http://www.hhs.gov/news/press/2012pres/09/20120917a.html [https://wayback.archive-it.org/3926/20150121155313/http://www.hhs.gov/news/press/2012pres/09/20120917a.html] (announcing the settlement).

117. *See Resolution Agreement Between HHS and Massachusetts Eye and Ear Infirmary*, HHS.GOV, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf (last visited September 20, 2016).

118. *See Resolution Agreement Between HHS and Massachusetts General Hospital*, HHS.GOV (Feb. 24, 2011) http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/massgeneralracap.pdf.

119. *See, e.g.*, 45 C.F.R. § 164.530(c)(1) (2016) ("A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."); *id*. § 164.306(a)(2), (3), and (4) (requiring covered entities to protect against "reasonably anticipated threats or hazards to the security or integrity of such information" "reasonably anticipated uses or disclosures of such information that are not permitted or required" by the Privacy Rule and to "[e]nsure compliance with the Security Rule by its workforce").

to draft sophisticated policies and procedures and conduct HIPAA-compliant training sessions for workforce members, but many covered entities are unable to fully operationalize all of the Privacy Rule's requirements due to their complexity.

Second, some covered entities value revenue generation over Privacy Rule compliance. Financially struggling hospitals and other covered entities can generate revenue by selling PHI to marketing companies, using and disclosing PHI for fundraising purposes, and entering into side businesses, including television show production. The problem is that most of these activities are prohibited by the Privacy Rule without prior written authorization and struggling covered entities may not obtain authorization before engaging in these lucrative practices.

Third, basic mobile technology and portable records issues continue to challenge privacy rule compliance. All of the HIPAA-compliant policies, procedures, and workforce trainings in the world cannot eliminate confidentiality breaches if workforce members do not adhere to such policies, procedures, and trainings, especially when handling mobile technology and portable records.