2013

Gone Too Far: Federal Regulation of Health Care Attorneys

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

STACEY A. TOVINO[*]

Gone Too Far: Federal Regulation of Health Care Attorneys

[*] Lincy Professor of Law and Associate Dean for Faculty Development and Research, William S. Boyd School of Law, University of Nevada, Las Vegas; Ph.D., University of Texas Medical Branch; J.D., University of Houston Law Center; B.A., Tulane University. I thank John Valery White, Executive Vice President and Provost, University of Nevada, Las Vegas, and Nancy Rapoport, Interim Dean and Gordon Silver Professor of Law, William S. Boyd School of Law, for their financial support of this research project. I also thank Chad Schatzle (Student Services Librarian, Wiener-Rogers Law Library), Emily Navasca (Research Assistant, Wiener-Rogers Law Library), Bryn Esplin (Research Assistant and President, Health Law Society, Boyd School of Law), and Kandis McClure (Research Assistant and Vice President, Health Law Society, Boyd School of Law) for their outstanding assistance in locating many of the sources referenced in this Article. I further thank the participants of the 65th Annual Meeting of the Southeastern Association of Law Schools in Amelia Island, Florida, and the participants of the 2011 Physicians and Physician Organizations Law Institute of the American Health Lawyers Association in Las Vegas, Nevada, for their helpful comments and suggestions on earlier drafts of this Article.

ABSTRACT

Outside health care counsel frequently obtain medical records, billing records, health insurance claims records, and other records containing individually identifiable health information in the course of representing health industry clients in medical malpractice, licensure, certification, accreditation, fraud and abuse, peer review, and other civil, criminal, and administrative health law matters. This Article is the first to argue that state rules of professional conduct, not federal health information confidentiality regulations, should govern outside health care counsel's use and disclosure of confidential client information, and that outside counsel should be excepted from direct federal regulation under the HIPAA Privacy Rule.

INTRODUCTION

Outside health care counsel frequently obtain medical records, billing records, health insurance claims records, and other records containing individually identifiable health information in the course of representing health industry clients in medical malpractice, licensure, certification, accreditation, fraud and abuse, peer review, and other civil, criminal, and administrative health law matters.[1] This Article examines the legal duties of confidentiality that apply to outside health care counsel who meet the definition of a business

[1] *See, e.g.*, Elizabeth C. Stone, *Attorney Access to Medical Records*, WIS. LAW., Oct. 2003, at 24, *available at* http://www.wisbar.org/AM/Template.cfm?Section=Wisconsin_Lawyer&template=/CM/ContentDisplay.cfm&contentid=49216 (discussing outside health care counsel's integral role in many aspects of their health care provider clients' operational matters); Elizabeth C. Stone, *Attorney Access To and Use of Medical Records*, WIS. LAW., Aug. 2003, at 18, *available at* http://www.wisbar.org/AM/Template.cfm?Section=Wisconsin_Lawyer&template=/CM/ContentDisplay.cfm&contentid=34198 (explaining that outside health care counsel frequently need access to their health care provider clients' medical records).

associate (BA) under federal health information confidentiality regulations (Privacy Rule),[2] giving special attention to the new duties imposed on BAs by the Health Information Technology for Economic and Clinical Health (HITECH) Act[3] within the American Recovery and Reinvestment Act (ARRA).[4]

This Article argues that HITECH's extension of the Privacy Rule directly to outside health care counsel who meet the definition of a BA is unjustified, illogical, and unnecessary, and will exacerbate existing conflicts of interest.[5] A proposed statutory amendment to HITECH would give the federal Department of Health and Human Services (HHS) the authority to except certain classes of BAs, including outside health care counsel, from direct regulation by the Privacy Rule as well as from the imposition of civil and criminal penalties.[6] Further proposals would preserve and strengthen the ability of state bars to impose sanctions on licensed attorneys who fail to maintain the confidentiality of client communications and records.[7]

Part I of this Article proceeds by reviewing the history of the Privacy Rule. Part II examines the obligations of confidentiality imposed by the pre-HITECH Privacy Rule: (1) directly on health plans, health care clearinghouses, and certain health care providers (covered entities); and (2) indirectly, by contract, on BAs, including many outside health care attorneys. Part III explores the new, direct duties of confidentiality that apply to BAs under HITECH as well as HHS's final modifications to the Privacy Rule implementing HITECH. Part IV summarizes the duties of confidentiality that apply to outside health care counsel under state rules of professional conduct.

Part V argues that HITECH's extension of the Privacy Rule directly to outside health care counsel who meet the definition of a BA is unjustified, illogical, and unnecessary, and will exacerbate existing conflicts of interest between health care attorneys and their clients. In particular, Part V.A. demonstrates that Congress had ample justification in 1996 for directing HHS to impose new confidentiality

---

2 45 C.F.R. §§ 164.500–164.534 (2011).

3 Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 115, 226–79 (2009).

4 American Recovery and Reinvestment Act (ARRA) of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

5 *See infra* Parts V.A.–C.

6 *See infra* Part VI.

7 *See id.*

requirements on health care providers and health plans given the *thousands* of providers and plans that failed to maintain the confidentiality of *millions* of patients and insureds. On the other hand, Part V.A also presents research showing that only a handful of cases involve claims against outside counsel for their alleged failure to maintain the confidentiality of their clients' individually identifiable health information, suggesting that the longstanding regulation of such attorneys by their state bars, as described in Part IV, may be more than sufficient. Part V.B. explores particular provisions within the Privacy Rule that HITECH extends directly to outside health care counsel, and demonstrates how the application of these provisions to outside health care counsel is illogical and unnecessary. Part V.B. also argues that, unlike state bars, HHS may not have the knowledge, skills, or experience necessary to regulate attorneys and other non-health industry participants. Part V.C. illustrates how HITECH's extension of the Privacy Rule to outside health care counsel will exacerbate existing conflicts of interest between outside health care counsel and their clients.

Part VI proposes that Congress amend HITECH to give HHS the authority to except certain classes of BAs, including outside health care counsel, from direct regulation by the Privacy Rule. Part VI offers language for the proposed statutory amendment and regulatory exception. Part VI also outlines methods for preserving and strengthening the ability of state bars to impose sanctions on licensed attorneys who fail to maintain the confidentiality of client information. This Article concludes with a recommendation that, going forward, Congress and HHS more carefully consider the application of health care-related regulations to non-health industry participants.

I
THE PRIVACY RULE: A BRIEF HISTORY

As signed into law by President Clinton on August 21, 1996, the Health Insurance Portability and Accountability Act (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.[8] The administrative simplification provisions, codified at Subtitle F of Title II of HIPAA, directed HHS to issue regulations protecting the privacy of individually identifiable health information if Congress failed to enact comprehensive privacy legislation within three years of HIPAA's enactment.[9] When Congress failed to meet its deadline, HHS incurred the duty to adopt privacy regulations.[10] HIPAA clarified, however, that any privacy regulations adopted by HHS must be made applicable only to three classes of covered entities: (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.[11]

HHS responded. On November 3, 1999,[12] and December 28, 2000,[13] HHS issued proposed and final rules, respectively, governing the confidentiality of protected health information ("PHI"). On March 27, 2002,[14] and August 14, 2002, [15] HHS issued proposed and final modifications to the Privacy Rule. With the exception of technical corrections and conforming amendments,[16] the Privacy Rule remained largely unchanged between 2002 and 2009.

---

[8] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 42 U.S.C.).

[9] *See id.* § 264(c)(1) ("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 . . . .").

[10] *See id.*

[11] *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 also generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,924 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160–64) [hereinafter Proposed HIPAA Privacy 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).

[12] Proposed HIPAA Privacy Rule, *supra* note 11, at 59,918.

[13] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160–64) [hereinafter Final HIPAA Privacy Rule].

[14] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (proposed modification Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

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

[16] *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 66 Fed. Reg. 12,434 (correction Feb. 26, 2001) (to be codified at 45 C.F.R. pts. 160, 164); Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information Published December 28, 2000, 65 Fed. Reg. 82,944 (correction Dec. 29, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

The nature and scope of the legal duties of confidentiality that applied to BAs, including many health care attorneys, changed significantly over three years ago. On February 17, 2009, President Obama signed ARRA into law.[17] Division A/Title XIII of ARRA, better known as HITECH, included certain privacy provisions that imposed new duties, and allowed for the imposition of civil and criminal penalties, directly on certain individuals who meet the definition of a BA under the Privacy Rule.[18]

Since ARRA's enactment, HHS has been busy issuing proposed, interim final, and final rules implementing HITECH's privacy-related requirements. On August 24, 2009, HHS released an interim final rule implementing HITECH's new breach notification requirements, including a breach notification requirement that applies directly to BAs.[19] 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.[20] On July 14, 2010, HHS released a proposed rule that would modify the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules in accordance with HITECH.[21] On May 31, 2011, HHS released a proposed rule that would modify the Privacy Rule's accounting of disclosures requirement.[22] On September 14, 2011, HHS released a proposed rule that would modify the Privacy Rule to provide individuals with the right to receive their laboratory test reports directly from the testing laboratories.[23] Finally,

---

17 ARRA, Pub. L. No. 111-5, 123 Stat. 115 (2009).

18 HITECH, Pub. L. No. 111-5, §§ 13001-13424, 123 Stat. 115, 226–279 (2009).

19 Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (interim Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160, 164).

20 HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (interim Oct. 30, 2009) (to be codified at 45 C.F.R. pt. 160) [hereinafter Enforcement Interim Final Rule].

21 Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160, 164).

22 HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31,426 (proposed May 31, 2011) (to be codified at 45 C.F.R. pt. 164) [hereinafter Proposed Accounting of Disclosures Rule].

23 CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports, 76 Fed. Reg. 56,712 (proposed Sept. 14, 2011) (to be codified at 42 C.F.R. pt. 493, 45 C.F.R. pt. 164).

on January 25, 2013, HHS released a final rule modifying the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules in accordance with HITECH (Final Modifications).[24] The proposals in this Article are especially timely given HHS's recent release of the Final Modifications.

II
PRE-HITECH DUTIES OF CONFIDENTIALITY

A. Direct Regulation of Covered Entities

As required by HIPAA, the pre-HITECH Privacy Rule directly regulated only the following covered entities: (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.[25] Although HHS indicated its desire to regulate all individuals and entities that receive or maintain individually identifiable health information, HHS also recognized that the rulemaking authority delegated to it by Congress in HIPAA was limited only to covered entities.[26]

The Privacy Rule directly regulates covered entities' uses of, disclosures of, and requests for individually identifiable health information to the extent such information does not constitute: (1) an education record protected under the Family Educational Rights and Privacy Act of 1974 (FERPA); (2) a student treatment record excepted from protection under FERPA; or (3) an employment record held by a covered entity in its role as an employer.[27] The name given by the Privacy Rule to the subset of individually identifiable health information described in the previous sentence is protected health information (PHI).

---

[24] 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 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164) [hereinafter Final Modifications].

[25] 45 C.F.R. § 160.103 (2011).

[26] Final HIPAA Privacy Rule, *supra* note 13, at 82,567.

[27] 45 C.F.R. § 160.103 (defining protected health information). The Final Modifications add a fourth category of information that is excluded from the definition of protected health information; that is, individually identifiable health information regarding a person who has been deceased for more than 50 years. *See* Final Modifications, *supra* note 24, at 5,689 (amending the definition of PHI at 45 C.F.R. § 160.103).

The Privacy Rule requires covered entities to adhere to a number of requirements when using and disclosing PHI.[28] For example, covered entities are allowed to freely use and disclose PHI for their "own treatment, payment, or health care operations."[29] Because "health care operations" is defined to include "legal services," covered entities may disclose PHI, including medical records, billing records, and health insurance claims records, to outside health care counsel for purposes of obtaining legal advice, counsel, and representation.[30]

Covered entities also 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.[31] These public policy activities include, but are not limited to, uses and disclosures required by law,[32] uses and disclosures for public health activities,[33] disclosures for law enforcement activities,[34] uses and disclosures for research,[35] and disclosures for workers' compensation activities.[36]

In the event that a covered entity would like to use or disclose PHI for a purpose that is not treatment, payment, health care operations, one of the public policy exceptions, or 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.[37] The Privacy Rule specifies the form of the authorization, including certain required elements and statements that are designed to place the individual on notice of how the individual's PHI will be used or disclosed.[38]

In addition to the use and disclosure requirements, the Privacy Rule also establishes five different individual rights.[39] These rights include the right of an individual to: (1) receive a notice of privacy

---

28 45 C.F.R. §§ 164.502–164.514 (establishing the use and disclosure requirements).

29 *Id.* § 164.506(c)(1).

30 *See id.* § 164.501; *see also* Final HIPAA Privacy Rule, *supra* note 13, at 82,596 (stating that a covered entity "may disclose relevant information to its attorneys, who are business associates, for purposes of health care operations, which includes uses and disclosures" necessary to obtain legal services).

31 45 C.F.R. § 164.512.

32 *Id.* § 164.512(a).

33 *Id.* § 164.512(b).

34 *Id.* § 164.512(f).

35 *Id.* § 164.512(i).

36 *Id.* § 164.512(l).

37 *See id.* § 164.508(a)(1).

38 *See id.* § 164.508(c)(1), (2).

39 *See id*. §§ 164.520–164.528.

practices,[40] (2) request additional privacy protections,[41] (3) access PHI,[42] (4) request amendment of incorrect or incomplete PHI,[43] and (5) receive an accounting of disclosures.[44]

Finally, the Privacy Rule establishes ten administrative requirements.[45] Pursuant to these administrative requirements, covered entities must: (1) designate a privacy officer and a contact person who are responsible for implementing the Privacy Rule and receiving and processing privacy-related complaints; (2) train their workforce members regarding the covered entity's privacy policies and procedures and the requirements of the Privacy Rule; (3) establish appropriate physical, technical, and administrative safeguards to protect the confidentiality of PHI; (4) provide a process for patients to make privacy-related complaints to the covered entity and the Secretary of HHS; (5) have and apply appropriate sanctions to members of the covered entity's workforce who violate the covered entity's privacy policies and procedures and the Privacy Rule; (6) mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI that violates the Privacy Rule; (7) not intimidate, threaten, coerce, discriminate, or otherwise retaliate against any individual who exercises any right available under the Privacy Rule; (8) not require patients to waive their rights under the Privacy Rule as a condition of receiving treatment; (9) implement policies and procedures designed to ensure compliance with the Privacy Rule; and (10) maintain such policies and procedures and other documentation required by the Privacy Rule for six years from the date when the documentation was created or the date when it last was in effect, whichever is later.[46]

---

[40] *Id.* § 164.520.

[41] *Id.* § 164.522.

[42] *Id.* § 164.524.

[43] *Id.* § 164.526.

[44] *Id.* § 164.528. HHS has proposed to give individuals an additional right; that is, the right to receive a written access report. Proposed Accounting of Disclosures Rule, *supra* note 22, at 31,448 (proposing new 45 C.F.R. § 164.528(b)(1), which would require covered entities to provide individuals with a written access report upon their request).

[45] 45 C.F.R. § 164.530.

[46] *Id.* § 164.530(a)–(j).

B. Indirect Regulation of Business Associates

Before HITECH, many individuals who did not meet the definition of a covered entity and who were not members of the workforce[47] of a covered entity continued to require access to PHI in order to perform functions, activities, and services for or on behalf of their covered entity clients. Third-party billing companies, for example, routinely receive PHI from their health care provider clients in order to create and send claims for reimbursement to health insurers.[48] Outside accountants and actuaries also require access to billing and claims records to provide accounting and actuarial services to their health care provider and health plan clients.[49] Pharmacy benefit managers similarly require access to claims records to provide pharmacy benefit management services to their health plan clients.[50] Before HITECH, these third-party billing companies, outside accountants and actuaries, pharmacy benefit managers, and other contractors fell within the definition of a BA and were not directly regulated by the Privacy Rule.

Attorneys who provide legal services to covered entities other than in the capacity of a workforce member of a covered entity also may require access to a covered entity's PHI in order to provide the requested legal services.[51] For example, an attorney who represents a physician in a medical malpractice claim will require a copy of the plaintiff's medical record to prove to a court that the care provided by

---

[47] Workforce means "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." *Id.* § 160.103. The Final Modifications expand the definition of workforce to include the workforce members of a business associate: "Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate." Final Modifications, *supra* note 24, at 5,689 (amending the definition of workforce at 45 C.F.R. § 160.103).

[48] Final HIPAA Privacy Rule, *supra* note 13, at 82,475, 82,476 (noting that billing firms require access to PHI of covered entity clients and therefore fall within the definition of a BA).

[49] *See id.* at 82,545 (noting that accountants require access to PHI to provide accounting services to their covered-entity clients).

[50] *See id.* at 82,466 (noting that covered entities frequently share PHI with pharmacy benefit managers to obtain their services).

[51] *See id.* at 82,596 (noting that attorneys need to use and disclose PHI in the course of representing their covered entity clients); *see also* JOHN R. CHRISTIANSEN, PREEYA M. NORONHA & BRAD M. ROSTOLSKY, BUSINESS ASSOCIATES IN A HITECH WORLD 13 (2011) (listing a number of situations in which outside counsel will fall within the definition of a BA).

the physician adheres to the standard of care. Similarly, an attorney who represents a hospital in an Emergency Medical Treatment and Active Labor Act (EMTALA)[52] claim will require copies of emergency room records documenting the medical screening examination and any necessary stabilizing treatment provided to the presenting patient in order to defend the hospital in a claim by the patient or the federal government.[53] Likewise, an attorney who represents a health care provider, health care supplier, or other individual or institution in a fraud and abuse action[54] may require access to medical records, billing records, and other records showing professional services rendered and insurance claims relating thereto. Moreover, an attorney who represents a physician or allied health professional in a hospital or other peer review matter[55] may require access to medical records containing entries authored by the health care provider. In all of these examples, an attorney who is not a workforce member of a covered entity requires access to PHI of the covered entity in order to properly advise, counsel, represent, or defend the covered entity and thus falls within the definition of a BA.[56] As discussed above and immediately below, the pre-HITECH Privacy Rule did not directly regulate the attorney's use or disclosure of the PHI. As discussed in more detail in Part III, HITECH now allows for the direct regulation of the attorney's use and disclosure of PHI by the federal government.

Before HITECH, the Privacy Rule did condition the disclosure of PHI by a covered entity to a BA on the covered entity's having a written agreement with the BA pursuant to which the BA agreed to maintain the confidentiality of the PHI received by the BA.[57] More

---

52 42 U.S.C. § 1395dd (2006).

53 *Id.* § 1395dd(a) (establishing a medical screening examination requirement); *id.* § 1395dd(b)(1) (establishing a necessary stabilizing treatment requirement).

54 Federal health care fraud and abuse authorities include the Anti-Kickback Statute, codified at 42 U.S.C. § 1320a-7(b), the Physician Self-Referral Law (also known as the Stark Law), codified at 42 U.S.C. § 1395nn, and the False Claims Act, codified at 31 U.S.C. § 3729 (2006).

55 The federal Health Care Quality Improvement Act (HCQIA) establishes procedures to be followed by hospitals when removing physicians from their medical staffs in order to qualify for immunity. 42 U.S.C. §§ 11111–11112. If a hospital fails to follow such procedures, the immunity provision may not apply and the physician may have a claim against the hospital under tort law, contract law, antitrust law, and other legal authorities. *Id.* § 11111.

56 *See* 45 C.F.R. § 160.103(1) (2011).

57 Final HIPAA Privacy Rule, *supra* note 13, at 82,504 ("We do not attempt to directly regulate business associates, but pursuant to our authority to regulate covered entities we

specifically, the Privacy Rule permitted a covered entity to disclose PHI to a BA only if the covered entity obtained satisfactory assurances from the BA that the BA would appropriately safeguard the PHI.[58] The pre-HITECH Privacy Rule required the covered entity to document the satisfactory assurances in a business associate agreement (BAA) that meets certain requirements.[59] The concepts of the BA and the BAA were considered a "work-around" of HHS's jurisdictional limitations under the HIPAA statute.[60]

The Privacy Rule required BAAs to contain several provisions.[61] First, unless both the covered entity and the BA are governmental entities, the BAA must establish the permitted and required uses and disclosures of such information by the BA.[62] Although HITECH slightly changed these requirements,[63] before HITECH, the BAA also must have provided that the BA would adhere to nine requirements, including: (1) not using or further disclosing the information other than as permitted or required by the BAA or as required by law; (2) using appropriate safeguards to prevent use or disclosure of the information other than as provided for by the BAA; (3) reporting to the covered entity any use or disclosure of the information not provided for by the BAA of which the BA becomes aware; (4) ensuring that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of, the covered entity agree to the same restrictions and conditions that apply to the BA with respect to such information;[64] (5) making available PHI in accordance with a Privacy Rule provision giving patients a right to access their PHI; (6) making available PHI for amendment and incorporating any amendments to PHI in accordance with a Privacy Rule provision giving patients the right to request amendment of incorrect or incomplete PHI; (7) making available information required to provide an accounting of disclosures

---

place restrictions on the flow of information from covered entities to non-covered entities.").

58 45 C.F.R. § 164.502(e)(1)(i).

59 *Id.* § 164.502(e)(2).

60 *See* CHRISTIANSEN ET AL., *supra* note 51, at 1.

61 45 C.F.R. § 164.502(e)(2).

62 *Id.* § 164.504(e)(2)(i).

63 *See infra* Part III.D.

64 The pre-HITECH requirement for a BA to ensure that any agents, including subcontractors, adhered to the same confidentiality restrictions and conditions that applied to the BA was (at least in practice) interpreted as a much looser standard than the regulatory requirement for BAAs. *See* CHRISTIANSEN ET AL., *supra* note 51, at 3.

in accordance with a Privacy Rule provision governing accountings of disclosures; (8) making its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, the covered entity available to the Secretary of HHS for purposes of determining the covered entity's compliance with the Privacy Rule; and (9) at termination of the contract, if feasible, returning or destroying all PHI received from, or created or received by the BA on behalf of, the covered entity that the BA still maintains in any form and retaining no copies of such information or, if such return or destruction is not feasible, extending the protections of the contract to the information and limiting further uses and disclosures to those purposes that make the return or destruction of the information infeasible.[65] Finally, the BAA must authorize termination of the BAA by the covered entity if the covered entity determines that the BA has violated a material term of the agreement.[66]

In summary, the pre-HITECH Privacy Rule did not directly regulate BAs, including many outside health care attorneys.[67] However, the pre-HITECH Privacy Rule indirectly regulated BAs by requiring covered entities to contractually obligate BAs to maintain the confidentiality of any PHI received by the BA.[68]

Before HITECH, a covered entity was considered not in compliance with the Privacy Rule if the covered entity knew of a pattern of activity or practice of the BA that constituted a material breach or violation of the BAA unless the covered entity took reasonable steps to cure the breach or end the violation.[69] If those steps were unsuccessful, the covered entity was required to "(A) [t]erminate the contract or arrangement, if feasible; or (B) [i]f termination [was] not feasible, report[] the problem to the Secretary [of HHS]."[70] A BA, including a covered entity's outside health care attorney, thus risked termination of both the BAA and the underlying representation agreement (and thus the privilege and benefits of representing the covered entity client) if the BA failed to maintain the

---

65 45 C.F.R. § 164.504(e)(2)(11)(A)–(I).

66 *Id.* § 164.504(e)(2)(111).

67 *See supra* Part II.A.

68 *See supra* text accompanying note 65; *see also* CHRISTIANSEN ET AL., *supra* note 51, at 3 ("While BAs could not be reached by HIPAA directly, they were reached indirectly by regulations which extended protections indirectly by requiring CEs to have a specific form of contract . . . in place before allowing their BA access to their PHI.").

69 45 C.F.R. § 164.504(e)(1)(11).

70 *Id.*

confidentiality of PHI received from the client. Before HITECH, however, a BA who failed to maintain the confidentiality of PHI did not risk the imposition of civil or criminal penalties by the federal government.

III
POST-HITECH DUTIES OF CONFIDENTIALITY

A. HITECH Overview

The nature and scope of the legal duties of BAs changed substantially on February 17, 2009, when President Obama signed ARRA, which includes HITECH, into law.[71] In terms of the duties of BAs, one of the most important provisions within HITECH is section 13404(a), which provides in relevant part: "The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity."[72] That is, certain provisions within the Privacy Rule now directly apply to BAs. Section 13404(a) is supported by HITECH section 13404(c), a second important provision within HITECH, which provides that the civil and criminal penalties set forth in the HIPAA statute (codified at Sections 1176 and 1177 of the Social Security Act) that heretofore only applied to covered entities now may be imposed directly on BAs who fail to maintain the confidentiality of their covered entity clients' PHI.[73] A third important HITECH provision is section 13402, which requires both covered entities and BAs, following the discovery of a breach of unsecured PHI ("uPHI"), to notify certain individuals and organizations of such breach.[74] HHS's implementation of these important HITECH sections is discussed in more detail below.

---

[71] ARRA, Pub. L. No. 111-5, 123 Stat. 115 (2009); HITECH, Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 115, 226–279 (2009).

[72] HITECH § 13404(a).

[73] *Id.* § 13404(c) ("In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6 [sic]) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act.").

[74] *See id.* § 13402.

B. Direct Regulation of Business Associates

Following the enactment of HITECH, many health care attorneys questioned how HHS would implement HITECH section 13404(a)'s requirement that privacy-related provisions be made applicable to BAs.[75] On January 25, 2013, HHS issued its Final Modifications, which show how broadly HHS interprets HITECH section 13404(a).[76]

More specifically, the preamble to the Final Modifications explains that HITECH section 13404(a): (1) creates direct liability for BAs when they use or disclose PHI other than in accordance with their BAAs, and (2) applies the other privacy requirements of HITECH to BAs just as they apply to covered entities.[77] To implement these HITECH changes, the Final Modifications significantly change the opening provisions of the Privacy Rule set forth at 45 C.F.R. sections 164.500, 164.502, and 164.504.[78]

In particular, the Final Modifications revise the first substantive regulation within the Privacy Rule to provide that the standards, requirements, and implementation specifications set forth in the Privacy Rule apply to a BA with respect to the PHI of a covered entity.[79] As discussed in more detail in Part V.B., this provision is somewhat illogical because most of the standards in the Privacy Rule only make sense when applied to health plans and health care providers, not non-health industry actors, including individual attorneys or law firms.[80] Stated another way, attorneys simply do not engage in treatment, health insurance reimbursement, health care utilization review, medical necessity reviews, determinations of health insurance eligibility or coverage, adjudication or subrogation of health benefit claims, risk adjustments based on a current or prospective insured's health status and demographic characteristics, training of health care professionals, health care quality assessment and improvement, development of clinical guidelines, health care

---

[75] *See id.* § 13404(a).

[76] Final Modifications, *supra* note 24, at 5,597.

[77] *Id.* at 5,597; *see also* Jennifer A. Stiller, *Lawyers Beware: Take Action Now to Protect Healthcare Information or Risk Stiff Penalties*, LAW OFFICES OF JENNIFER A. STILLER (Feb. 1, 2010), http://www.healthregs.com/HITECH-HIPAA-BusinessAssociate Rules.shtml (explaining that HITECH requires attorneys who represent physicians, hospitals, health insurance companies, and other Covered Entities to directly comply with the Privacy Rule).

[78] Final Modifications, *supra* note 24, at 5,695–97.

[79] *Id.* at 5,695 (amending 45 C.F.R. § 164.500(c)).

[80] *See infra* Part V.B.

protocol development, case management and care coordination, health care professional peer review, medical training of health care professionals, health insurance underwriting, health insurance premium rating, public health activities, biomedical and behavioral research, and most other activities that are regulated by the standards, requirements, and implementation specifications set forth in the Privacy Rule.

In addition, the Final Modifications revise the Privacy Rule's second substantive regulation to generally provide that a BA, like a covered entity, may not use or disclose PHI except as permitted or required by the Privacy Rule or the HIPAA Enforcement Rule.[81] For example, if an outside health care attorney who meets the definition of a BA sells a patient's PHI without obtaining the prior written authorization of the patient who is the subject of the PHI, the attorney would be violating the Privacy Rule. By further example, if an outside health care attorney who meets the definition of a BA inappropriately uses, discloses, or requests more than the minimum amount of PHI that is necessary to provide legal services to the covered entity, the attorney also would be violating the Privacy Rule. As discussed in more detail in Part V.A., this provision is also somewhat unnecessary because, unlike *the tens of thousands* of documented cases of confidentiality breaches by health plans and health care providers, research revealed *only a handful* of cases in which outside counsel breached the confidentiality of their covered entities' PHI. In addition, state rules of professional conduct already prohibit attorneys from using and disclosing client records for inappropriate purposes.

The Final Modifications also add new sub-provisions within the second substantive regulation to specifically address the permitted and required uses and disclosures of PHI by BAs.[82] For example, one provision allows BAs to use or disclose PHI only as permitted or required by their BAAs or as required by law.[83] Thus, if an outside health care attorney who constitutes a BA uses or discloses PHI for a purpose other than the purposes (e.g., legal and other professional services) specified in the BAA, the attorney would be violating the Privacy Rule.

A second provision clarifies that a BA is not permitted to use or disclose PHI in a manner that would violate the requirements of the

---

81 Final Modifications, *supra* note 24, at 5,696 (amending 45 C.F.R. § 164.502(a)).

82 *Id.* (adding 45 C.F.R. § 164.502(a)(4)).

83 *Id.* (adding 45 C.F.R. § 164.502(a)(3)).

Privacy Rule if done by a covered entity.[84] Thus, if it would be a violation of the Privacy Rule for a covered hospital to sell a patient's PHI without the patient's authorization, it would also be a violation of the Privacy Rule for the covered hospital's outside health care counsel to sell a hospital patient's PHI without the patient's authorization.

A third provision obligates BAs to disclose PHI in certain situations. For example, the Final Modifications obligate BAs to disclose PHI to the covered entity, the patient or insured who is the subject of the PHI, and/or the patient's designee, as necessary to satisfy the covered entity's obligations relating to the individual's right to inspect and obtain a copy of his or her PHI.[85] Thus, if a patient requests a covered hospital to give the patient access to her PHI and the covered hospital's outside health care attorney, for some reason, has PHI that the covered hospital does not (a highly unlikely hypothetical), the attorney would be required under the Final Modifications to provide PHI to the covered hospital or the individual to facilitate the individual's right of access to her PHI.

A fourth provision modifies the minimum necessary standard to require that when BAs use, disclose, or request PHI, they must limit the PHI to the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure, or request.[86] Stated another way, a BA is not making a permitted use or disclosure under the Privacy Rule if the BA does not apply the minimum necessary standard, where appropriate.[87] An outside health care attorney who constitutes a BA should be mindful of the Final Modifications when requesting copies of medical records, billing records, claims information, or other information that the attorney needs in order to provide legal services to a covered entity client. If the attorney needs only a discrete class of information in order to provide the requested legal services, the attorney has a regulatory obligation to limit her request to that discrete class of information. On the other hand, many civil and criminal defense attorneys need access to entire record sets in order to identify facts that could support the application of a particular legal defense, such as contributory negligence, comparative negligence, or assumption of the risk, in the medical malpractice context. If a defense attorney requires an entire

---

84 *Id.* (adding 45 C.F.R. § 164.502(a)(3)).

85 *Id.* (amending 45 C.F.R. § 164.502(a)(4)(ii)).

86 *Id.* at 5,697 (amending 45 C.F.R. § 164.502(b)(1)).

87 *See id.* at 5,597.

record or record set to properly represent or defend a covered entity, the attorney may continue to request the entire record or record set.

HHS amended the minimum necessary provisions to specifically reference the obligation of a BA to only use, disclose, or request the minimum amount of information necessary to accomplish the intended purpose. However, HHS did not add references to BAs to other provisions of the Privacy Rule that now apply to BAs. In the preamble to the Final Modifications, HHS reasons that because the Final Modifications prohibit a BA from using or disclosing PHI in any manner that would violate the Privacy Rule if done by a covered entity, additional references to BAs in the Privacy Rule's use and disclosure requirements are unnecessary: "[A]ny Privacy Rule limitation on how a covered entity may use or disclose [PHI] automatically extends to [BAs]."[88]

C. Civil Penalties, Criminal Penalties, and Audits

HITECH provides that the civil and criminal penalties set forth in the HIPAA statute and codified at sections 1176 and 1177 of the Social Security Act now apply to BAs who violate any provision of HITECH sections 13404(a) and 13404(b).[89] On October 30, 2009, HHS released an interim final rule implementing strengthened enforcement provisions for the Privacy Rule, including strengthened civil monetary penalties.[90] In addition, HHS released the Final Modifications implementing HITECH's directed changes to the Enforcement Rule on January 25, 2013. The Final Modifications clarify (by adding the phrase "business associate" to many provisions within the Administrative Simplification regulations) that the Secretary of HHS may impose civil money penalties not only on Covered Entities but also on BAs who violate the Privacy Rule.[91] This means that the Secretary may impose civil money penalties on outside health care attorneys who meet the definition of a BA and violate the Privacy Rule.[92]

---

[88] *Id.*

[89] HITECH, Pub. L. No. 111-5, § 13404(c), 123 Stat. 115, 264 (2009).

[90] Enforcement Interim Final Rule, *supra* note 20, at 56,123.

[91] *See, e.g.*, Final Modifications, *supra* note 24, at 5,691 (amending 45 C.F.R. § 160.402(a) to provide that "the Secretary will impose a civil money penalty upon a covered entity *or business associate* if the Secretary determines that the covered entity *or business associate* has violated an administrative simplification provision" (emphasis added)).

[92] For violations of the Privacy Rule occurring on or after February 18, 2009, the Secretary may impose civil money penalties of $100 to $50,000 (if the BA did not know,

Outside health care attorneys who meet the definition of a BA also may be subject to criminal penalties. Criminal penalties remain at their pre-HITECH levels, including: (1) criminal fines of not more than $50,000, imprisonment of not more than one year, or both; (2) for offenses committed under false pretenses, criminal fines of not more than $100,000, imprisonment of not more than five years, or both; and (3) for offenses committed "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," criminal fines of not more than $250,000, imprisonment of not more than ten years, or both.[93]

Finally, HITECH section 13411 provides that BAs shall be subject to periodic audits by the Secretary of HHS as one way of ensuring that BAs are complying with their new privacy-related requirements.[94]

IV
DUTIES OF CONFIDENTIALITY UNDER STATES RULES OF PROFESSIONAL CONDUCT

The previous Parts examined the indirect and direct confidentiality requirements imposed by the original Privacy Rule and HITECH, respectively, on health care attorneys who meet the definition of a BA. This Part examines the legal duties of confidentiality imposed on all licensed attorneys, including licensed outside health care counsel, by state rules of professional conduct. Under the American Bar Association's (ABA's) Model Rules of Professional Conduct (Model Rules) and state rules of professional conduct, all licensed attorneys have an ethical duty to maintain the confidentiality of client information acquired during the course of, or by reason of representation of, a client.[95] The rule of confidentiality applies not

---

and by exercising reasonable diligence would not have known, of the violation); of $1,000 to $50,000 (if the violation was due to reasonable cause and not willful neglect); of $10,000 to $50,000 (if the violation was due to willful neglect and was corrected during the first 30 days); and of $50,000 (if the violation was due to willful neglect and was not corrected during the first 30 days). *See* Final Modifications, *supra* note 24, at 5,583 (charting the different penalty levels). However, civil money penalties may not exceed $1.5 million for identical violations in a calendar year regardless of the BA's level of culpability. *Id.*

93 42 U.S.C. § 1320d-6 (2012).

94 HITECH § 13411.

95 *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2011); TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 1.05(b) (West, Westlaw through 2012 amendments).

only to matters communicated to the attorney in confidence by the client, but also to all information relating to the representation, whatever its source.[96] Medical records, billing records, and other information and data obtained by a health care attorney while representing a patient or health industry client constitutes "confidential information" for purposes of rules of the professional responsibility.[97]

Except as otherwise permitted, most state rules prohibit an attorney from knowingly revealing confidential information of a client or former client to: (1) a person that the client has instructed is not to receive the information; or (2) any other person, other than the client, the client's representatives, or the members, associates, or employees of the attorney's law firm.[98] These rules would prohibit, for example, a health care attorney from disclosing the contents of medical or billing records obtained during the course of representation to the attorney's spouse, partner, or friends, or to other third parties for purposes unrelated to the legal advice and counsel for which the attorney was retained.

Most state rules of professional conduct also prohibit an attorney from: (1) using confidential information of a client to the disadvantage of the client unless the client consents after consultation; (2) using confidential information of a former client to the disadvantage of the former client after the representation is concluded unless the former client consents after consultation or the confidential information has become generally known; or (3) using privileged information of a client for the advantage of the attorney or of a third person, unless the client consents after consultation.[99] These rules would, of course, prohibit a health care attorney from selling medical record or other patient or insured data to a newspaper or tabloid for

---

[96] *See, e.g.*, *In re* Disciplinary Proceedings Against Harman, 628 N.W.2d 351, 361 (Wis. 2001).

[97] *See, e.g.*, *id.* (adjudicating a disciplinary action taken by then-named Wisconsin Board of Attorneys Professional Responsibility (Board) against a Wisconsin-licensed attorney for his failure to maintain the confidentiality of his client's medical records; the Board suspended the attorney's license to practice law for six months after finding, among other things, that the client "did not authorize [the attorney] to release her medical records to anyone. [The attorney's] disclosure of information that he obtained while representing [the client] violated client-lawyer confidentiality"; the Wisconsin Supreme Court further explained that "the rule of client-lawyer confidentiality applies not only to matters communicated in confidence by the client, . . . but also to all information relating to the representation whatever its source.'").

[98] *See, e.g.*, TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 1.05(b)(1).

[99] *See, e.g.*, *id.* R. 1.05(b)(2)–(4).

the financial advantage of the attorney or to the disadvantage of the attorney's health industry client.

Most state rules of professional conduct permit an attorney to reveal unprivileged client information in certain situations, including: (1) when impliedly authorized to do so in order to carry out the representation; and (2) when the attorney has reason to believe it is necessary to do so in order to: (i) carry out the representation effectively; (ii) defend the attorney or the attorney's employees or associates against a claim of wrongful conduct; (iii) respond to allegations in any proceeding concerning the attorney's representation of the client; or (iv) prove the services rendered to a client, or the reasonable value thereof, or both, in an action against another person or organization responsible for the payment of the fee for services rendered to the client.[100] These rules would thus permit an attorney who specializes in medical malpractice to use medical record data in petitions, answers, counterclaims, motions and other pleadings as necessary to bring or defend a health care liability claim.

Most state rules of professional conduct also permit an attorney to reveal confidential information acquired during the course of or reason of representation of a client: (1) when the attorney has been expressly authorized to do so in order to carry out the representation; (2) when the client consents after consultation; (3) to the client, the client's representatives, or the members, associates, and employees of the attorney's firm, except when otherwise instructed by the client; (4) when the attorney has reason to believe it is necessary to do so in order to comply with a court order, a state rule of professional conduct, or other law; (5) to the extent reasonably necessary to enforce a claim or establish a defense on behalf of the lawyer in a controversy between the lawyer and the client; (6) to establish a defense to a criminal charge, civil claim or disciplinary complaint against the attorney or the attorney's associates based upon conduct involving the client or the representation of the client; (7) when the attorney has reason to believe it is necessary to do so in order to prevent the client from committing a criminal or fraudulent act; and (8) to the extent revelation reasonably appears necessary to rectify the consequences of a client's criminal or fraudulent act in the commission of which the attorney's services had been used.[101] Health care attorneys routinely rely on some of these exceptions to

---

[100] *See, e.g., id.* R. 1.05(d)(1)–(2).

[101] *See, e.g., id.* R. 1.05(c)(1)–(8).

confidentiality. For example, the third clause in the previous sentence permits a senior partner or shareholder who is representing a health industry client to share medical records, billing records, and other individually identifiable health information with a junior associate, paralegal, or other law firm employee who is needed by the senior partner to assist in the representation of the client.

An attorney's state law duty of confidentiality to a client is grounded in the fiduciary duty owed by the attorney to the client as well as the need for the legal system to function properly.[102] Without an assurance of confidentiality, a health industry client may fail to seek early legal assistance or fully disclose the facts of the matter to her attorney.[103] An attorney's duty of confidentiality is given effect not only in state rules of professional conduct but also in the law of evidence regarding the attorney-client privilege as well as through the law of agency.[104] The attorney-client privilege, for example, provides patients and health industry clients the right to prevent certain confidential communications from being revealed by compulsion of law.[105]

In summary, the provisions governing confidentiality in most state rules of professional conduct are comprehensive and detailed. The provisions explain exactly when an attorney can and cannot use and disclose confidential client information, and carefully balance a client's need for confidentiality with the attorney's need to use and disclose information to carry out the representation. Unlike the Privacy Rule, there are no provisions governing confidentiality in the state rules that are nonsensical when applied to attorneys. All of the permissions and prohibitions set forth in the state rules govern activities that come up on a daily basis in an attorney's practice. These state rules, drafted by attorneys for attorneys, should govern an attorney's use and disclosure of confidential client information.

V
ARGUMENTS AGAINST HITECH'S EXTENSION OF THE PRIVACY RULE TO OUTSIDE HEALTH CARE COUNSEL

This Part argues that HITECH's extension of the Privacy Rule's confidentiality requirements directly to outside health care counsel

---

102 *See, e.g., id.* R. 1.05 cmt. 1.

103 *See, e.g., id.*

104 *See, e.g., id.* R. 1.05 cmt. 3.

105 *See, e.g., id.*

who meet the definition of a BA is unjustified, illogical, and unnecessary, and will exacerbate existing conflicts of interest between health care attorneys and their health industry clients.

A. HITECH's Extension of the Privacy Rule to Outside Health Care Counsel Is Unjustified

Congress's initial decision in 1996 to directly regulate health plans, health care clearinghouses, and certain health care providers was well justified. First, remember that Congress's purpose in enacting HIPAA's Administrative Simplification provisions was to improve the Medicare and Medicaid programs (two covered health plans), as well as the efficiency and effectiveness of the health care system more generally by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.[106] Congress also recognized, however, that the increased accessibility of health information made possible by the widespread and growing use of electronic media by health plans and health care providers, as well as the new federal mandate for standard transactions and code set use by health plans and health care providers, would require enhanced confidentiality requirements.[107] No such federal mandate for standard transaction and code set use[108] was applied to BAs, including outside health care counsel. Without a requirement to electronically transmit health information, there was no resulting increase in the risk of a confidentiality breach by such BAs, including outside health care counsel.

---

[106] 42 U.S.C. § 1320d-2 (2012). At the time of HIPAA's enactment, approximately 400 different health insurance claim formats were in use in the United States. The submission of electronic health care claims was limited, then, because most health care providers could support only a handful of formats. In order to improve the efficiency and effectiveness of the health care system, Congress directed HHS to create uniform standards for health insurance-related transactions as well as uniform codes (called 'standard transactions and code sets') to be used in those transactions. *See* William P. Matthews, *Caught Up In the Expanding Net: Regulation of the Business Associate Under the HIPAA Privacy Regulations*, J. KAN. B. ASS'N, Apr. 2003, at 32, 33 (explaining the need for standard transactions and code sets).

[107] Proposed HIPAA Privacy Rule, *supra* note 11, at 59,928; *see also* Alex L. Bednar, *HIPAA Implications for Attorney-Client Privilege*, 35 ST. MARY'S L.J. 871, 880 (2004) (discussing the legislative history of HIPAA, including the belief of some legislators that electronic technology innovation would increase privacy and security concerns).

[108] *See supra* note 106 and accompanying text (explaining standard transactions and code sets).

Like Congress, HHS also recognized that the growing use of computerization in the health care industry, including the rapid growth of electronic transfers of health information between and among health plans, health care clearinghouses, and health care providers, gave rise to significant confidentiality concerns:[109]

> [M]ore and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information. In 1996, the health care industry invested an estimated $10 billion to $15 billion on information technology . . . . The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button.[110]

HHS further explained that the number of health care industry participants that maintain and transmit individually identifiable health information has increased over the last decade: "The health care industry has been transformed from one that relied primarily on one-on-one interactions between patients and clinicians to a system of integrated health care delivery networks and managed care providers."[111]

HHS's concerns were supported by relevant findings of the American Health Information Management Association (AHIMA).[112] According to AHIMA, approximately 150 health care providers and ancillary hospital service providers—including physicians, nurses, x-ray technicians, and billing clerks—"have access to a patient's medical records during the course of a typical hospitalization."[113]

According to other research organizations, such as the National Research Council, health care providers and plans frequently shared individually identifiable health information with consulting physicians, managed care organizations, health insurance companies, life insurance companies, self-insured employers, pharmacies, pharmacy benefit managers, clinical laboratories, accrediting organizations, state and federal statistical agencies, and medical information bureaus.[114] Although some of these individuals and organizations had a legitimate need to access, use, and disclose medical, billing, and claims records, over-sharing such information

---

109 Proposed HIPAA Privacy Rule, *supra* note 11, at 59,928.

110 Final HIPAA Privacy Rule, *supra* note 13, at 82,465.

111 *Id.* at 82,466.

112 *Id.*

113 *Id.*

114 *Id.*

increased the risk that patients' confidential information would be leaked to outside sources. However, at that time, there were no federal statutes or regulations governing which classes of individuals could access, use, and disclose these records, what information in the records should and could be accessed, used, and disclosed, and the use and disclosure restrictions that should attach to such information.

Concerns about the lack of attention to health information confidentiality by health care providers, health plans, and other health care industry participants were not just theoretical.[115] In 1993, Johnson & Johnson, the New Jersey-based multi-national manufacturer of pharmaceutical, diagnostic, therapeutic, surgical, and biotechnology products, marketed a list of five million names and addresses of elderly incontinent women without their permission.[116] In 1996, an employee of the Tampa, Florida, health department removed from her work a computer disk containing the names of 4,000 people who had tested positive for HIV.[117] In 1999, a Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet.[118] In 2000, a Utah-based pharmaceutical benefit management firm used patient data to solicit business for its owner, a drug store.[119] The same year, a patient in a Boston-area hospital discovered that her medical records had been read by more than 200 of the hospital's employees.[120]

Even after the April 14, 2003, general compliance date for the HIPAA Privacy Rule,[121] health care providers and health plans continued to inappropriately use and disclose PHI. For example, between 2005 and 2008, numerous members of the workforce of covered health care provider UCLA Health System repeatedly and without permission examined the electronic PHI of UCLA patients.[122] By further example, between 2005 and 2009, covered health care provider Phoenix Cardiac Surgery failed to have in place appropriate and reasonable administrative and technical safeguards to protect the

---

115 *Id.* at 82,467.

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.*

120 *Id.*

121 45 C.F.R. § 164.534 (2011).

122 Written Resolution Agreement and Corrective Action Plan 08-82727 and 08-83510 between the U.S. Department of Health and Human Services, Office for Civil Rights, and the Regents of the University of California, 1–2 (July 6, 2011), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/uclahsracap.pdf.

confidentiality of PHI, which contributed to the posting of over 1,000 separate entries of ePHI on a publicly accessible, Internet-based calendar and the daily transmission of ePHI from an Internet-based email account to workforce members' personal Internet-based email accounts.[123]

On several occasions in 2006, Rite Aid pharmacies located in cities across the United States disposed of paper PHI in open dumpsters potentially accessible to persons who were not members of Rite Aid's workforce.[124] Television media actually videotaped Rite Aid pharmacy workforce members disposing of prescriptions and labeled pill bottles containing patient identifiable information in industrial trash containers that were accessible to the general public.[125] Similarly, and on several occasions in 2006 and 2007, CVS pharmacies located in cities across the United States also disposed of paper PHI in open dumpsters potentially accessible to persons who were not members of CVS's workforce.[126] Media outlets also caught the CVS disposals on videotape.[127]

Some of the covered health plans and health care providers who were inappropriately using and disclosing PHI were doing so for marketing purposes. Between 2007 and 2010, for example, covered entity Management Services Organization Washington, Inc. (MSO) impermissibly disclosed PHI to Washington Practice Management

---

123 *See* Written Resolution Agreement and Corrective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and Phoenix Cardiac Surgery, P.C., 2 (Apr. 13, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.

124 *See* Written Resolution Agreement and Collective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and Rite Aid Corporation, 1 (June 7, 2010), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/riteaidres.pdf.

125 *See Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/riteaidresagr.html (last visited Jan. 26, 2013).

126 *See* Written Resolution Agreement and Corrective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and CVS Pharmacy, Inc., 2 (Jan. 15, 2009), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresagrcap.pdf.

127 *See Resolution Agreement*: *CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html (last visited Aug. 20, 2012).

(WPM) without a valid authorization to enable WPM to market Medicare Advantage plans to those individuals.[128]

Some covered health plan and health care provider disclosures were due to theft. In 2009, for example, covered health plan Blue Cross Blue Shield of Tennessee (BCBST) discovered a theft of computer equipment, including 57 hard drives believed to contain over one million health plan member names, identification numbers, diagnosis codes, dates of birth, and social security numbers.[129] The data stolen also included over 300,000 video recordings and over one million audio recordings containing patient identifiable information.[130] BCBST internal investigation confirmed that the PHI of 1,023,209 individuals was stored on the hard drives.[131] Also in 2009, an Alaska Department of Health and Social Services computer technician had a portable electronic device potentially containing ePHI stolen from his vehicle.[132]

Some inappropriate disclosures by covered health plans and health care providers were caused by the behavior of just one covered entity employee. In 2009, for example, a Massachusetts General Hospital (MGH) employee removed from MGH premises documents containing PHI so that the employee could work from home.[133] The PHI consisted of billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of provider of 66 patients and the practice's daily office schedules for three days containing the names and medical

---

128 *See* Written Resolution Agreement and Corrective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and Management Services Organization Washington, Inc., 1 (Dec. 13, 2010), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/msoresultionagreement.pdf.

129 Written Resolution Agreement and Corrective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and BlueCross BlueShield of Tennessee, 1–2 (Mar. 9, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_cap.pd.

130 *Id.* at 1.

131 *Id.* at 2.

132 Written Resolution Agreement and Corrective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and Alaska Department of Health and Social Services, 1 (June 25, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf.

133 Written Resolution Agreement and Corrective Action Plan between the U.S. Department of Health and Human Services, Office for Civil Rights, and The General Hospital Corporation and Massachusetts General Physicians Organization, Inc., 1 (Feb. 14, 2011), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralracap.pdf [hereinafter MGH Resolution Agreement].

record numbers of 192 patients[134] of MGH's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS.[135] Three days later, when the employee was commuting back to work on the subway, the employee removed the records containing PHI from her bag and placed them on the seat beside her.[136] Upon exiting the subway, the MGH employee left the documents on the subway train and they were never recovered.

As of July 31, 2012, OCR had investigated and resolved 17,025 cases of Privacy Rule violations by requiring changes in privacy practices and other corrective actions by covered health plans and health care providers.[137] The most common types of covered entities that were required to take corrective action to achieve voluntary compliance were, in order of frequency: private medical practices, general hospitals, outpatient facilities, health plans (including group health plans and health insurance issuers), and pharmacies.[138]

In summary, Congress's initial decision in 1996 to directly regulate health plans, health care clearinghouses, and certain health care providers was well justified. Before and after the compliance date for the Privacy Rule, *thousands* of health industry participants had inappropriately used and disclosed the PHI of *millions* of patients and insureds.[139]

Even though thousands of health industry participants inappropriately used and disclosed the PHI of millions of patients and insureds, the question is whether there is any evidence that outside health care counsel also were (or are) inappropriately using or disclosing PHI received from their health industry clients. Because HHS did not directly regulate outside health care counsel and other BAs prior to HITECH, HHS would not be the source of such information, at least such information dating prior to HITECH. After HITECH, when Congress gave HHS the statutory authority to directly

---

134 *Id.*

135 *Resolution Agreement*: *Massachusetts General Hospital Settles Potential HIPAA Violations*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralra.html (last visited Jan. 26, 2013).

136 MGH Resolution Agreement, *supra* note 133, at 1.

137 *See Enforcement Highlights (as of July 31, 2012)*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/07312012.html (follow "Enforcement Results as of the Date of This Summary" hyperlink) (last visited Jan. 26, 2013).

138 *Id.*

139 *See supra* text accompanying notes 116 to 138.

regulate BAs[140] and gave state attorneys general the statutory authority to take action against covered entities and BAs in their states who inappropriately used and disclosed PHI,[141] research revealed only one action against a BA. However, that BA was not an attorney. On July 31, 2012, Minnesota Attorney General Lori Swanson (AG) announced that business associate Accretive Health, Inc., a Chicago-based debt collector that managed the revenue operations of several Minnesota hospitals, was being forced to cease operations in the State of Minnesota under a settlement of the AG's federal lawsuit against Accretive.[142] One of the reasons for the AG's lawsuit was the discovery that an Accretive laptop containing data on over 23,000 patients of two Minnesota covered hospitals was stolen from the rental car of an Accretive employee.[143] Accretive's failure to maintain the confidentiality of its client hospitals' PHI does not suggest that attorneys as a class are unable to maintain client confidentiality.

Another source of information regarding the inappropriate use or disclosure of PHI by BAs might be states that, through state health information confidentiality laws that are similar to the federal Privacy Rule, apply directly to BAs. Since its enactment in 2001, for example, the Texas Medical Records Privacy Act (Texas Act) has always directly regulated Covered Entities, BAs, and any other person who comes into possession of, obtains, or stores PHI.[144] That is, the Texas

---

140 *See* HITECH, Pub. L. No. 111-5, § 13404(a), 123 Stat. 115, 264 (2009) ("The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate . . . ."). The date by which BAs must comply with their new obligations under the Final Modifications is September 23, 2013. Final Modifications, *supra* note 24, at 5,566. Therefore, HHS has not yet taken action against a BA for its failure to comply with the Final Modifications.

141 *See* HITECH § 13410(e) ("[I]n any case in which the attorney general of a State has reason to believe than an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of this part, the attorney general of the State, as parens patriae, may bring a civil action on behalf of such residents of the State in a district court of the United States of appropriate jurisdiction . . . .").

142 *Attorney General Swanson Says Accretive Will Cease Operations in the State of Minnesota Under Settlement of Federal Lawsuit*, OFFICE OF ATTORNEY GEN. LORI SWANSON (July 31, 2012), http://www.ag.state.mn.us/Consumer/PressRelease/07312012AccretiveCeaseOperations.asp.

143 *Id.*

144 *See* TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2)(A)–(D) (West, Westlaw through 2011 Sess.); *see also* Bednar, *supra* note 107, at 906 (explaining that "[t]he result of [the Texas Act's overbroad language] is that countless persons with no direct relationship to health care are statutorily liable for safeguarding PHI in Texas").

Act has always directly regulated outside health care counsel who receive medical records, billing records, and other records containing PHI from their health industry clients. Enforcement of the Texas Act includes injunctive relief,[145] civil penalties,[146] investigation and disciplinary actions,[147] and attorney general action.[148] Effective September 1, 2012, the Texas Legislature the civil penalties that may be imposed on BAs and other individuals who violate the Texas Act; that is, civil penalties may be assessed up to: (1) $5,000 per violation that is committed negligently; (2) $25,000 per violation that is committed knowingly or intentionally; (3) $250,000 per violation that is committed intentionally and if PHI is used for financial gain; and (4) $1.5 million if a "pattern or practice" is found.[149] As of this writing, research revealed no injunctions, civil penalties, investigative or disciplinary actions, or attorney general actions taken against any Texas-licensed attorneys (or any other BAs, for that matter) for their failure to maintain the confidentiality of PHI received from their covered entity clients in accordance with the Texas Act.

Another source of information regarding the possible inappropriate use or disclosure of PHI by outside health care counsel would be cases in which state-licensed health-care attorneys had been accused by a state agency of violating state rules of professional conduct that require attorneys to maintain the confidentiality of client communications, as described in Part IV of this Article. Research revealed only two published opinions in cases in which a state agency accused an attorney of failing to maintain the confidentiality of PHI received from a client.

In *In re Harman*, Wisconsin-licensed attorney Donald Harman was accused by the Wisconsin Board of Attorneys Professional Responsibility (Board) of a number of rule violations, including mishandling client funds, representing a client in the presence of a conflict of interest without obtaining a written consent of the conflict, knowingly disobeying an obligation of tribunal rules, using information obtained during the representation of a former client to that former client's disadvantage, and revealing information relating

145 TEX. HEALTH & SAFETY CODE ANN. § 181.201(a).

146 *Id.* § 181.201(b).

147 *Id.* § 181.202.

148 *Id.* § 181.201(e).

149 *Id.* § 181.201(b)(1)–(3), (c).

to the representation of the client without the client's consent.[150] With respect to the final allegation, Harman was consulted by a client about a potential legal malpractice action against another attorney who had formerly represented the client in a medical malpractice action.[151] In connection with the potential legal malpractice representation, Harman obtained the former attorney's files, including the client's medical records, which contained information about the client's drug and alcohol dependence and history of self-abusive behavior.[152] Without the client's consent, Harman disclosed the client's drug and alcohol dependence and history of self-abusive behavior to a Wisconsin county district attorney who was prosecuting the client's former boyfriend for domestic abuse of the client.[153]

The Supreme Court of Wisconsin held that Harman violated Rule 1.6(a) of the Wisconsin Rules of Professional Conduct for Attorneys when he disclosed the client's drug and alcohol dependence and history of self-abusive behavior to the district attorney.[154] The court explained: "[I]t is a 'fundamental principle' in the client-lawyer relationship that the lawyer maintain confidentiality of 'information relating to the representation.'"[155] The court further explained: "[T]he rule of client-lawyer confidentiality applies not only to matters communicated in confidence by the client, '. . . but also to all information relating to the representation whatever its source.'"[156] The court upheld the board's recommendation that Harman's license to practice law be suspended for six months.[157]

Far from suggesting that outside health care counsel as a class routinely make inappropriate uses or disclosures of PHI, the *Harman* case suggests that one general practice attorney who had a lengthy history of professional conduct problems (this was Harman's fourth disciplinary action) may need more stringent sanctions imposed on him by his state bar. The case also illustrates, however, a weakness associated with the use of the post-HITECH Privacy Rule as a mandate for attorney confidentiality. The post-HITECH Privacy Rule

---

150 *See In re* Disciplinary Proceedings Against Harman, 628 N.W.2d 351, 354 (Wis. 2001).

151 *Id.* at 358.

152 *Id.*

153 *Id.*

154 *Id.* at 361.

155 *Id.* at 361.

156 *Id.*

157 *Id.*

only protects a patient's PHI when it is in the hands of an attorney who represents a covered entity, such as a health care provider or health plan. When an attorney represents a patient or insured, the post-HITECH Privacy Rule does not regulate the attorney's use or disclosure of the PHI because the patient or insured does not fall within the definition of a covered entity. This Article argues that a patient's or insured's health information should not have fewer confidentiality protections simply because the attorney who maintains the information is directly representing the patient or insured instead of the patient's or insured's health care provider or health plan. State rules of professional conduct, by contrast, appropriately require adherence to rules of confidentiality by all attorneys, including attorneys who represent health care providers and health plans as well as attorneys who represent patients and insureds.

In addition to *In re Harman*, research revealed only one other published opinion in which a state agency accused an attorney of failing to maintain the confidentiality of PHI received from a client. In *In re Mullins*, Indiana-licensed attorney Patty Sue Mullins was accused by the Indiana Supreme Court Disciplinary Commission of violating Rule 1.6 of the Indiana Rules of Professional Conduct for Attorneys at Law (Indiana Rule 1.6), which prohibits lawyers from revealing confidential client information.[158] As background, the parents of an Indiana woman who was in a persistent vegetative state had petitioned an Indiana court for authority to compel the woman's health care providers to withdraw the woman's artificially-administered hydration and nutrition based on the parents' belief that the daughter would never recover from her brain injury.[159] Mullins, who disagreed with the parents' plan, created an Indiana corporation named the Christian Fellowship with the Disabled, Inc. (Fellowship) and filed on behalf of the Fellowship a petition that would appoint Mullins as temporary guardian of the woman based on Mullins's belief that the woman was being medically neglected due to her lack of hydration and nutrition.[160] After a court appointed Mullins as temporary guardian, Mullins faxed portions of the woman's medical records to several news media outlets throughout Marion County, Indiana, apparently in an attempt to justify Mullins's involvement in the litigation.[161]

---

158 *In re* Mullins, 649 N.E.2d 1024, 1025 (Ind. 1995).

159 *Id.* at 1025.

160 *Id.*

161 *Id.*

The Supreme Court of Indiana held that Mullins violated Indiana Rule 1.6, reasoning that "no legitimate or recognized justification for [Mullins's] county-wide dissemination of the records" existed.[162] The Court further explained that the woman's medical record was "information relating to representation of a client" within Indiana Rule 1.6 and that "[a] lawyer must make every effort practicable to avoid unnecessary disclosure of information relating to a representation, [and] to limit disclosure to those having a need to know it."[163] In light of Mullins's lack of prior disciplinary actions, her devotion of significant time and energy during her legal career to public causes, and her lack financial or other sinister motives, the court ordered only public reprimand and admonishment.[164]

The *Mullins* case is a second example of a general practice attorney, not a health care attorney, who inappropriately disclosed a client's PHI. Like *Harman*, the *Mullins* case also illustrates a weakness associated with the use of the post-HITECH Privacy Rule as a mandate for attorney confidentiality. Again, the post-HITECH Privacy Rule would not have regulated Mullins because Mullins was representing a patient, not a covered entity. And, again, this Article argues that a patient's health information should not have fewer confidentiality protections simply because the attorney who maintains that information is directly representing the patient instead of the patient's health care provider. State rules of professional conduct, including the Indiana Rules of Professional Conduct for Attorneys at Law, appropriately require adherence to rules of confidentiality by all attorneys, including attorneys who represent health care providers as well as attorneys who represent patients.

In addition to the two published opinions in *Harman* and *Mullins*, research also revealed one unpublished opinion in which a state agency accused an attorney of failing to maintain the confidentiality of PHI received from a client. In *Statewide Grievance Committee v. Paige*, the Connecticut Statewide Grievance Committee (Committee) accused Connecticut-licensed attorney Sheri Paige of violating eight different Connecticut Rules of Professional Conduct, including Rule 1.6 relating to the confidentiality of client information, in connection with the representation of a client with respect to his application for

---

162 *Id.* at 1025.

163 *Id.* at 1026.

164 *Id.*

immigration to the United States.[165] In particular, when Paige provided the individual with a list of information that would assist Paige in processing the immigration application, the list was handwritten on the reverse side of a piece of paper that contained medical information relating to another client of Paige's.[166] The medical information included the name of the client's treating physician and the details of the physician's medical bill.[167] The Superior Court of Connecticut held that "[b]y allowing access to this confidential information, [Paige] violated Rule 1.6(a)."[168] Given Paige's significant prior disciplinary history, the number of rule violations associated with the instant representation, and the lack of any mitigating factors, the court suspended Paige from the practice of law for a period of one year.[169] As in *Harman* and *Mullins*, the *Statewide Grievance Committee* case would not have implicated the post-HITECH Privacy Rule because Paige inappropriately disclosed the PHI of a client who was a patient, not a covered entity.

Another source of information regarding the possible inappropriate use or disclosure of PHI by outside health care counsel would be cases in which private plaintiffs accused their health care providers or health plans' outside health care counsel of inappropriately using or disclosing PHI. Research revealed only one relevant case. In *Biddle v. Warren General Hospital*, several patients brought a class action against a hospital and its outside law firm, alleging that the hospital inappropriately disclosed PHI to the law firm to enable the law firm to search for Supplemental Security Income (SSI) eligibility for the payment of patients' unpaid medical bills.[170] In addition to holding that an independent tort exists for the unauthorized, unprivileged disclosure of confidential information by the hospital to the law firm,[171] the Supreme Court of Ohio also held that the law firm could be held independently liable for inducing the hospital's unauthorized and tortious disclosure of information to the firm.[172] The court reasoned that the attorney's need for the information (including the

---

165 Statewide Grievance Comm. v. Paige, No. CV030198335S, 2004 WL 1833462, at *2–3 (Conn. Super. Ct. July 14, 2004).

166 *Id.* at *2.

167 *Id.* at *7.

168 *Id.* at *7.

169 *Id.* at *9.

170 Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 518 (Ohio 1999).

171 *Id.* at 523.

172 *Id.* at 528.

attorney's desire to benefit the patients by making them eligible for SSI) was irrelevant unless the need also advanced or protected some interest giving rise to a privilege.[173] The court further reasoned that the only interest that had been recognized in such regard was the patient's interest in obtaining medical care and treatment, and that disclosure would be limited to those who have a legitimate interest in the patient's health.[174] In the end, the court held that the law firm could be held liable for inducing the hospital's unauthorized, unprivileged disclosure of nonpublic medical information learned within the context of the physician-patient relationship.[175]

Unlike the attorneys in *Harman*, *Paige*, and *Statewide Grievance Committee*, the law firm in *Biddle* was using and disclosing the PHI of a covered entity; that is, a hospital. The law firm in *Biddle* thus would have been regulated by the Privacy Rule had the facts in *Biddle* not occurred in the mid-1990s, almost a decade before the 2003 compliance date for the pre-HITECH Privacy Rule and fifteen years prior to HITECH's extension of the Privacy Rule directly to BAs. However, even if the case had occurred later in time, the Privacy Rule would have allowed the hospital and law firm to use and disclose the patients' PHI without their prior authorization in order to determine SSI eligibility; that is, the Privacy Rule expressly permits covered entities and their BAs to use and disclose PHI for certain "payment" activities and the definition of "payment" includes determinations of insurance eligibility and coverage.[176] In summary, Ohio tort law, not the Privacy Rule, would have prohibited the hospital and law firm's activities.

Other than *Harman*, *Paige*, *Statewide Grievance Committee*, and *Biddle*, research revealed no other cases in which a state-licensed attorney was accused by a state agency in an administrative action or a client in a private tort action of inappropriately using or disclosing PHI received from the client. This Article assumes that our careful research missed a few cases that did not contain standard search terms such as "attorney!," "lawyer!," "counsel!," "law firm!," "law practice," "medical record!", "health record!," "health information," "confidential!," "privacy," "private," and "Rule 1.6," but that did

---

173 *Id.*

174 *Id.*

175 *Id.*

176 45 C.F.R. § 164.506(c)(1) (2011) ("A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations."); *id.* § 164.501 (defining "payment" to include "[d]eterminations of eligibility or coverage").

involve an allegation by a state agency or a private plaintiff against an attorney or law firm for the failure to maintain the confidentiality of PHI. Even assuming a 500 percent error rate in our research, research would reveal twenty or fewer judicial opinions involving cases in which outside counsel failed to maintain the confidentiality of PHI. Twenty cases of inappropriate uses and disclosures of PHI by outside counsel probably do not justify Congress and HHS's decision to extend the Privacy Rule when compared to the *thousands* of covered entities who inappropriately used and disclosed the PHI of *millions* of patients and insureds.

Assuming for the moment that Congress and HHS had sufficient justification for extending the Privacy Rule directly to attorneys who constitute BAs, note that in three of the four cases described above the Privacy Rule would not have regulated (or deterred) the conduct described because the defendant attorneys in those cases failed to maintain the PHI of clients who were patients, not covered entities. In the fourth case, *Biddle*, the Privacy Rule would now regulate the defendant law firm's use and disclosure of the PHI it received from its covered hospital client; however, the Privacy Rule explicitly authorizes the use and disclosure of PHI for the SSI eligibility purposes described in *Biddle*. In summary, the extension of the Privacy Rule directly to attorneys who meet the definition of a BA would not have made any difference to the outcomes of the four identified cases in which an attorney allegedly inappropriately used and disclosed PHI.

Compared to state rules of professional conduct described in Part IV, the Privacy Rule thus has several weaknesses. First, the Privacy Rule only regulates attorneys who represent covered entities, whereas state rules of professional conduct appropriately regulate all attorneys with respect to their use and disclosure of confidential client information. Second, the Privacy Rule allows some information uses and disclosures disallowed by state rules of professional conduct and complained of by patients like the plaintiffs in *Biddle*.

B. HITECH's Extension of the Privacy Rule to Outside Health Care Counsel Is Illogical and Unnecessary

As discussed in Part III, HITECH makes BAs adhere to the same Privacy Rule use and disclosure requirements that apply to covered

entities.[177] The problem is that the Privacy Rule's use and disclosure requirements were designed for health industry participants and are illogical when applied to attorneys.[178] For example, the Privacy Rule allows Covered Entities to freely use and disclose PHI for their own treatment, payment, and related health care operations activities.[179] Health care providers use PHI to treat their patients, health plans use PHI to determine whether and how much to pay for such treatments, and both health care providers and health plans engage in dozens of related health care operations activities, so this particular use and disclosure allowance makes a great deal of sense in the health care setting. Attorneys do not treat patients or request payment for treating patients, (and to do so would constitute the unlicensed and criminal practice of medicine[180] as well as state and federal health care fraud and abuse[181]) so the regulatory allowance for treatment and payment activities usually does not make sense in the legal setting. In fact, other than "legal services," which is included in the fourth paragraph of the six-paragraph definition of "health care operations,"[182] attorneys do not engage in, or perform on behalf of their covered entity clients, most of the other activities that are regulated by the standards, requirements, and implementation specifications set forth in the Privacy Rule. These activities include, but are not limited to, patient referrals, patient consultations, health care utilization review, medical necessity reviews, risk adjustments based on a current or prospective insured's health status and demographic characteristics, training of health care professionals, health care quality assessment and improvement, development of clinical guidelines, health care protocol development, case management and care coordination,

---

177 HITECH, Pub. L. No. 111-5, § 13404(a), 123 Stat. 115, 264 (2009) ("The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate . . . ."); Final Modifications, *supra* note 24, at 5,696 (adding 45 C.F.R. § 164.502(a)(3)) (stating that a BA is not permitted to use or disclose PHI in a manner that would violate the requirements of the Privacy Rule if done by a covered entity).

178 *See infra* text accompanying notes 179–89.

179 45 C.F.R. § 164.506(c)(1).

180 *See, e.g.*, TEX. OCC. CODE ANN. § 155.001 (West, Westlaw through 2011 Reg. Sess.) (prohibiting an individual from practicing medicine without a license to practice medicine); *id.* § 165.151(a) (making the unlicensed practice of medicine a criminal offense in the State of Texas).

181 *See, e.g.*, 31 U.S.C. § 3729 (2006) (codifying the federal False Claims Act prohibition of the submission of health care claims by individuals not licensed to provide health care).

182 45 C.F.R. § 164.501.

health care professional peer review, medical training of health care professionals, health insurance underwriting, health insurance premium rating, public health activities, biomedical and behavioral research.[183] In summary, other than generally prohibiting attorneys from inappropriately using or disclosing PHI, which state rules of professional conduct already prohibit,[184] the provisions in the Final Modifications[185] are nonsensical when applied to attorneys.

On the other hand, ABA Model Rule 1.6 (and analogous provisions within state rules of professional conduct) was designed expressly for attorneys. Each provision within a state rule of professional conduct makes sense when applied to an attorney with respect to the attorney's use or disclosure of confidential client information. Typically, the main confidentiality provision requires all licensed attorneys to maintain the confidentiality of client information acquired during the course of, or by reason of representation of, a client, applies regardless of whether the client is a covered entity or not.[186] Typically, the main provision applies not only to matters communicated to the attorney in confidence by the client but also to all information relating to the representation, whatever its source, and regardless of whether the information was obtained from a covered entity or a non-covered entity.[187] All medical records, billing records, and other information and data obtained by an attorney while representing a covered entity or non-covered entity thus constitutes "confidential information" for purposes of rules of professional responsibility.[188] In addition, the ABA Model Rules and most state

---

183 *Id.* §§ 164.501–164.514 (regulating a variety of health care related uses and disclosures of PHI).

184 *See supra* Part IV (summarizing the confidentiality obligations of attorneys under state rules of professional conduct).

185 *See* Final Modifications, *supra* note 24, at 5,695 (adding new 45 C.F.R. § 164.500(c), stating: "Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.").

186 *See, e.g.*, TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 1.05(a) (West, Westlaw through 2012 amendments).

187 *See, e.g.*, *In re* Disciplinary Proceedings Against Harman, 628 N.W.2d 351, 361 (Wis. 2001).

188 *See, e.g.*, *id.* (discussing a disciplinary action taken by then-named Wisconsin Board of Attorneys Professional Responsibility (Board) against a Wisconsin-licensed attorney for his failure to maintain the confidentiality of his client's medical records; the Board suspended the attorney's license to practice law for six months after finding, among other things, that the client "did not authorize [the attorney] to release her medical records to anyone. [The attorney's] disclosure of information that he obtained while representing [the client] violated client-lawyer confidentiality"; the Wisconsin Supreme Court further

rules of professional conduct list situations in which an attorney may disclose otherwise confidential client information.[189] Unlike the Privacy Rule's exceptions for uses and disclosures of PHI for treatment, payment, health care operations, and public policy activities which, for the most part, are illogical when applied to attorneys, the permissions set forth in state rules of professional conduct make sense when applied to attorneys.

The extension of the Privacy Rule directly to outside counsel is illogical for other reasons. For example, it is not clear that HHS has the knowledge, skill, expertise, or resources to regulate attorneys. Through its ten health-related operating divisions, including the Administration for Children and Families, the Administration for Community Living, the Agency for Healthcare Research and Quality, the Centers for Disease Control and Prevention, the Centers for Medicare & Medicaid Services, the Food and Drug Administration, the Health Resources and Services Administration, the Indian Health Service, the National Institutes of Health, and the Substance Abuse and Mental Health Services Administration,[190] HHS's stated mission is to protect the health of all Americans and to provide essential human services, especially for those who are least able to help themselves.[191] HHS's expertise, by its own admission, is in the

---

explained that, "[T]he rule of client-lawyer confidentiality applies not only to matters communicated in confidence by the client, ' . . . but also to all information relating to the representation whatever its source.'").

189 *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2011) ("A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: (1) to prevent reasonably certain death or substantial bodily harm; (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services; (3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services; (4) to secure legal advice about the lawyer's compliance with these Rules; (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; (6) to comply with other law or a court order; or (7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.").

190 *HHS Leadership: Operating Divisions*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/open/contacts/index.html#od (last visited Jan. 28, 2013).

191 *About HHS*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/about/ (last visited Jan. 28, 2013).

provision of health and human services to individuals who need health care and social services,[192] not in the provision of legal advice to clients with legal problems or in the regulation or discipline of attorneys.

Unlike HHS, each state bar has special expertise in the practice of law, the requirements for the professional and ethical practice of law, and the regulation of attorneys in that state.[193] Indeed, one of the stated missions of most state bars is to assure that the public is protected and served by attorneys and other legal services providers who meet the highest standards of competence and ethics, including standards relating to client confidentiality.[194] All state bars are governed by a board of directors, governors, or trustees, the majority of the members of which usually are attorneys who are also licensed to practice law in that state and thus are familiar with the ethical and legal requirements to which attorneys must adhere, including requirements relating to client confidentiality.[195] All state bars have a discipline system that is designed to protect the public, the courts, and the profession from attorneys who violate ethical rules covering their professional conduct.[196] Given the extremely small number of cases in which state-licensed attorneys have been accused by their clients or state bars of the inappropriate use and disclosure of PHI,[197] this Article suggests that: (1) state bars are appropriately educating attorneys regarding the importance of client confidentiality; (2) the sanctions that state bars may impose on non-compliant attorneys,

---

192 *Id.* ("The Department of Health and Human Services (HHS) is the United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves.").

193 *See, e.g.*, *The State Bar of California Overview*, STATE BAR OF CAL., http://www.calbar.ca.gov/AboutUs/StateBarOverview.aspx (last visited Sept. 1, 2012) [hereinafter *State Bar of California*].

194 *See, e.g.*, *id.* (describing the mission of the State Bar of California); *Our Mission at the State Bar of Texas*, STATE BAR OF TEX., http://www.texasbar.com/AM/Template.cfm?Section=Our_Mission&Template=/CM/HTMLDisplay.cfm&ContentID=19576 (last visited Jan. 28, 2013) (outlining the mission of "foster[ing] high standards of ethical conduct for lawyers, enabl[ing] its members to better serve their clients and the public"); Our Mission, STATE BAR OF NEV., http://www.nvbar.org/content/our-mission (last visited Jan. 28, 2013) ("Our Mission is to govern the legal profession, to serve our members, and to protect the public interest. Our Goals are . . . to uphold and elevate the standard of honor, integrity, and courtesy in the legal profession . . . .").

195 *See, e.g.*, *State Bar of California*, *supra* note 193 (describing governance in the state bar in relevant section of page).

196 *See, e.g.*, *id.* (describing the state's attorney discipline system in relevant section of page).

197 *See supra* text accompanying notes 140–57.

including fines, license suspension, and license revocation, are serving as appropriate deterrents against breaches of confidentiality involving PHI; and/or (3) attorneys learned in law school, through required coursework in Professional Responsibility classes, the importance of client confidentiality and have applied that learning to protect client records that include PHI.

In summary, HITECH's extension of Privacy Rule principles to outside health care counsel is somewhat illogical and unnecessary given: (1) the lack of evidence that attorneys inappropriately use or disclose their covered entities' PHI; (2) the fact that most of the Privacy Rule is illogical when applied to attorneys; (3) the fact that the only Privacy Rule provisions that make sense when applied to attorneys are the general provisions that prohibit BAs from using or disclosing PHI for non-permitted purposes;[198] (4) the fact that state rules of professional conduct already prohibit attorneys from using or disclosing PHI for non-legal and other inappropriate or non-permitted purposes; and (5) the fact that HHS has stated expertise in the provision of health and human services, not in the practice of law, the regulation of attorneys, or the discipline of attorneys.

C. HITECH'S Extension of the Privacy Rule to Outside Health Care Counsel Will Exacerbate Existing Conflicts of Interest

HITECH's extension of the Privacy Rule to outside health care counsel also will exacerbate existing conflicts of interest. As background, an attorney generally is prohibited from representing a client if the representation involves a concurrent conflict of interest.[199] Under the ABA's Model Rules, a concurrent conflict of interest exists when either: (1) the attorney's representation of one client will be directly adverse to another client; or (2) there is a significant risk that the representation of one or more clients will be materially limited by the attorney's responsibilities to another client, a former client, or a third person, or by a personal interest of the lawyer.[200]

---

198 *See* 45 C.F.R. § 164.504(e)(2)(i) (requiring BAAs to "[e]stablish the permitted and required uses and disclosures of such information by the business associate" and prohibiting the BAA from authorizing the BA to further use or disclose the PHI in a manner that would violate the Privacy Rule if done by the covered entity); Final Modifications, *supra* note 24, at 5,696 (adding new 45 C.F.R. § 164.502(a), stating: "A . . . business associate may not use or disclose protected health information, except as permitted or required by [the Privacy Rule or the Breach Notification Rule]").

199 *See* MODEL RULES OF PROF'L CONDUCT R. 1.7(a) (2011).

200 *Id.*

Although the Privacy Rule and HITECH do not pit one covered entity against another in a way that would implicate the first provision, there is a risk that an outside health care counsel's representation of a covered entity, when the outside counsel is required to enter into a BAA with that same covered entity, would be materially limited by the personal interests of the outside counsel. That is, in drafting the BAA between the covered entity and itself, the outside counsel would have an interest in minimizing its obligations under the BAA whereas the covered entity would desire provisions, such as indemnification provisions and limitation of liability provisions, that would protect the covered entity in the case of the outside counsel's own breach of confidentiality involving the covered entity's PHI.[201]

In addition, under the pre-HITECH Privacy Rule, the outside counsel was required to agree through the BAA to report to the covered entity any inappropriate uses or disclosures of the covered entity's PHI of which the BA became aware, including the outside counsel's own inappropriate uses and disclosures.[202] Because the BAA was required to authorize the covered entity to terminate the BAA (and therefore the underlying representation agreement) if the covered entity determined that the BA violated a material term of the agreement,[203] and because the outside counsel's reporting of its own inappropriate uses and disclosures to the covered entity could result in the covered entity's termination of the BAA (and therefore the underlying representation agreement), the outside counsel had a personal interest in not reporting any confidentiality violations to the covered entity.

HITECH exacerbates these conflicts of interest due to its creation of four new breach notification requirements. First, HITECH requires covered entities to notify each individual whose uPHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of a breach.[204] Second, HITECH requires covered entities to notify prominent media outlets serving a

---

201 *See, e.g.*, Alan Stuart Goldberg, *HIPAA, HITECH Act, Attorneys, and Business Associates: Professional Conduct Contracting Requirements Are Expanding–Are You Ready Now?* VA. STATE BAR, 3, 5 (Mar. 29, 2010), http://www.vsb.org/docs/sections/health/hipaahitech2010130929032010.pdf (discussing the potential conflicts of interest that exist when an attorney represents a covered entity and enters into a BAA with that covered entity, and the specific conflicts associated with indemnification provisions).

202 45 C.F.R. § 164.504(e)(2)(iii).

203 *Id.*

204 HITECH, Pub. L. No. 111-5, § 13402(a), 123 Stat. 115, 260 (2009).

state or jurisdiction following the discovery of a breach of uPHI involving more than 500 residents of such State or jurisdiction.[205] Third, HITECH requires covered entities to: (1) immediately notify the Secretary of HHS following the discovery of a breach of uPHI involving 500 or more individuals; and (2) create and maintain a log of breaches involving less than 500 individuals and annually submit such log to the Secretary.[206] Fourth, HITECH imposes additional breach notification requirements directly on BAs. That is, HITECH requires a BA who discovers a breach of uPHI to notify the covered entity of the breach without unreasonable delay and in no case later than sixty calendar days after the discovery of a breach.[207]

If outside counsel (or one of counsel's employees, agents, or subcontractors) is the source of a confidentiality breach, counsel would have an incentive not to notify its appropriate covered entity client of such breach, in accordance with the fourth breach notification requirements above, because counsel would risk: (1) the covered entity's termination of the BAA (and, thus, the underlying representation agreement),[208] which would result in a loss to counsel of the covered entity's legal business; (2) the covered entity's reporting of the breach to the individuals who are the subject of the information,[209] which could lead to private lawsuits against counsel based on the disclosure tort, as in the *Biddle* case;[210] (3) the covered entity's reporting of the breach to prominent media outlets,[211] which could be damaging to counsel's business and personal reputation; and (4) the covered entity's reporting of the breach to the Secretary,[212] which could trigger an audit and lead to the imposition of civil and criminal penalties directly against counsel.[213] In summary, HITECH's breach notification requirements create additional risks that counsel's representation of the covered entity would be limited by counsel's own interest in not reporting confidentiality breaches in order to avoid the loss of legal business, future tort lawsuits, damage to counsel's

---

205 *Id.* § 13402(e)(2).

206 *Id.* § 13402(e)(3).

207 *Id.* § 13402(b); Final Modifications, supra note 24, at 5,695 (adopting 45 C.F.R. § 164.410(b)).

208 *See supra* text accompanying note 203.

209 *See supra* text accompanying note 204.

210 *See* Biddle v. Warren Gen. Hosp., 715 N.E.2d 518 (Ohio 1999); *see also supra* text accompanying notes 170–75.

211 *See supra* text accompanying note 205.

212 *See supra* text accompanying note 206.

213 *See supra* Part III.C.

reputation, government audits, and government-imposed civil and criminal penalties.

It is also possible that outside counsel will discover a Privacy Rule violation by the covered entity. Although the breach notification rules do not require BAs to report covered entity violations to the individuals who are the subject of the information, the media, or HHS (so conflicts are not created due to any such mandatory notification obligations), outside counsel certainly would want to avoid complicity with the violation, especially because violations can give rise to civil and criminal penalties for both covered entities and BAs. Counsel who know of a Privacy Rule violation by a client covered entity will thus face several ethical and professional questions, including whether to represent the covered entity in any civil or criminal action by the federal government or whether to withdraw from representation due to a conflict, such as outright complicity or a more subtle desire to minimize evidence of counsel's own contributions to the Privacy Rule violation and to provide evidence to the government suggesting that the covered entity had greater fault.

Finally, as discussed in Part III.C, HITECH section 13411 provides that BAs shall be subject to periodic audits by the Secretary of HHS as one way of ensuring that BAs are complying with their new, direct, privacy-related requirements.[214] The new statutory allowance for auditing of BAs may be problematic from the perspective of the covered entity because there is some precedent stating that production of law firm records in response to government audits may waive both the attorney-client privilege as well as work-product doctrine protection.[215]

Notwithstanding the existence of a concurrent conflict of interest, an attorney may start or may continue to represent a client under the Model Rules, but only if four criteria are satisfied: First, the attorney must reasonably believe that he or she will be able to provide "competent and diligent representation" to the covered entity; second, the representation must not be "prohibited by law"; third, the representation must not involve the "assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal"; finally, each affected client must give "informed consent, confirmed in writing."[216]

---

214 HITECH, Pub. L. No. 111-5, § 13411, 123 Stat. 115, 276 (2009).

215 CHRISTIANSEN ET AL., *supra* note 51, at 20.

216 MODEL RULES OF PROF'L CONDUCT R. 1.7(b) (2011).

Although the second and third criteria should be non-issues in this context, the first and fourth criteria do require further consideration. The outside counsel must reasonably believe that he or she will be able to provide competent and diligent representation to the covered entity and the covered entity must give written, informed consent to the conflict of interest. That is, the outside counsel must recognize: (1) the incentives he or she will have to not include language in the BAA that is favorable to the covered entity (and unfavorable to the BA), such as indemnification or limitation of liability provisions; (2) that he or she will have an incentive not to report its own confidentiality lapses and breaches to the covered entity; (3) that in an investigation by HHS into a breach that possibly involved both the covered entity and the outside counsel, that counsel would have an incentive to minimize its own contributions and blame the violation on the covered entity; and (4) that any audit of itself by HHS could result in waiver of both the attorney-client privilege as well as work-product doctrine production. Given these recognitions, counsel would have to make a determination that he or she would still be able to provide competent and diligent representation to the covered entity. In addition, counsel would need to disclose all of these potential conflicts to the covered entity in writing and obtain the covered entity's consent to such conflicts. In summary, HITECH exacerbates existing conflicts of interest between outside health care counsel and covered entities.

VI
A LEGISLATIVE AND REGULATORY PROPOSAL

In light of the argument that HITECH's extension of the Privacy Rule's confidentiality requirements directly to outside health care counsel who meet the definition of a BA is unjustified, illogical, and unnecessary, and will exacerbate existing conflicts of interest between outside health care counsel and their clients, the final question is whether HITECH's imposition of direct confidentiality duties on BAs should be challenged, retained, or disposed of. It is unlikely that a challenge by an individual attorney, group of attorneys, or law-related professional association, such as the ABA, with respect to HITECH's extension of the Privacy Rule to attorneys would be successful. In *American Bar Association v. Federal Trade Commission*, the ABA and the New York State Bar Association (NYSBA) challenged the direct application of the confidentiality-related requirements within the federal Gramm-Leach-Bliley Act (GLBA) to attorneys, reasoning

that the GLBA did not give the Federal Trade Commission (FTC) jurisdiction to regulate state-licensed attorneys.[217] As background, effective in 1999, the GLBA imposed comprehensive confidentiality obligations on financial institutions with respect to their clients' nonpublic personal information.[218]

The United States Court of Appeals for the D.C. Circuit agreed with the ABA and NYSBA and held that state-licensed attorneys engaged in the practice of law were not "financial institutions" within the GLBA's provisions that required protection of consumer financial information.[219] The court reasoned:

> The states have regulated the practice of law throughout the history of the country; the federal government has not. This is not to conclude that the federal government could not do so. We simply conclude that it is not reasonable for an agency [the FTC] to decide that Congress has chosen such a course of action in [GLBA statutory] language that is, even charitably viewed, at most ambiguous.[220]

It is unlikely that a challenge similar to the challenge in *American Bar Association v. Federal Trade Commission* would be effective with respect to HITECH. Unlike the statutory provisions within the GLBA, which did not extend authority to the FTC to regulate attorneys as financial institutions, the statutory provisions within HITECH specifically require the direct regulation of BAs.[221]

In a later lawsuit, the ABA challenged the FTC's application of the federal Fair and Accurate Credit Transactions (FACT) Act to attorneys.[222] As background, the FACT Act amended the Fair Credit Reporting Act to authorize the FTC to promulgate regulations requiring financial institutions and creditors to establish internal procedures to prevent identity theft.[223] In 2007, the FTC adopted identity theft rules (Red Flags Rules) that required such "financial institutions and creditors to implement and maintain programs to protect consumers from identity theft."[224] Neither the FACT Act nor

---

217 *See* Am. Bar Ass'n v. Fed. Trade Comm'n, 430 F.3d 457, 458 (D.C. Cir. 2005).

218 *Id.* at 459.

219 *Id.* at 470–71.

220 *Id*. at 472.

221 HITECH, Pub. L. No. 111-5, § 13404(a), 123 Stat. 115, 264 (2009) ("The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate . . . .").

222 Am. Bar Ass'n v. Fed. Trade Comm'n, 636 F.3d 641, 643 (D.C. Cir. 2011).

223 *Id.*

224 *Id.*

the Red Flag Rules specified whether the Red Flags Rules applied to attorneys.[225] In 2009, in response to public confusion regarding the application of the Red Flags Rules, "the FTC issued an Extended Enforcement Policy, explaining that 'professionals, such as lawyers or health care providers, who bill their clients after services are rendered,' would be considered 'creditors' under the [FACT Act] and therefore, subject to the [Red Flags] Rule's requirements."[226] Shortly thereafter, the ABA sued, challenging the FTC's Extended Enforcement Policy on the grounds that the FTC had intruded upon the practice of law, an area of traditional state regulation.[227] Due to the enactment of subsequent legislation addressing the precise issue before the court in favor of the ABA, the court ultimately dismissed the case as moot.[228]

In summary, there is precedent for a legal challenge to the direct regulation of state-licensed attorneys by federal agencies; however, such legal challenges were supported by a lack of statutory authority for the extension of federal requirements to attorneys. In the instant case, HITECH specifically states Congress' desire to directly regulate BAs.[229]

The next question is whether the confidentiality duties imposed by HITECH on BAs who are attorneys should be retained together with the confidentiality duties imposed on attorneys under State Rules of Professional Conduct (with the Privacy Rule's preemption provisions governing differences between the two sets of authorities). HHS knew when it drafted the Privacy Rule that other confidentiality schemes existed under state law and that the Privacy Rule would need to be reconciled with such other confidentiality schemes to the extent such authorities conflicted.[230] To that end, HHS included within the Privacy Rule a provision specifying that, in general, the Privacy Rule

---

225 *Id.*

226 *Id.*; *see also* FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, 16 C.F.R. § 681.1, 1 n.2 (2008) ("For example, creditors under the ECOA [Equal Credit Opportunity Act] include professionals, such as lawyers or health care providers, who bill their clients after services are rendered.").

227 *Am. Bar Ass'n*, 636 F.3d at 643.

228 *Id.* at 649.

229 *See supra* text accompanying note 221.

230 *See How Does the HIPAA Privacy Rule Reduce the Potential for Conflict with State Laws?*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/faq/preemption_of_state_law/401.html (last visited Jan. 29, 2013).

preempts contrary state laws.[231] A state law will survive preemption, however, if the state law relates to the privacy of individually identifiable health information and is more stringent than the relevant Privacy Rule provision.[232] Among other examples, a state law would be more stringent than a Privacy Rule provision if: (1) with respect to a use or disclosure, the state law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under the Privacy Rule; or (2) the state law provides greater privacy protection for the individual who is the subject of the PHI.[233]

One of the reasons for the Privacy Rule's preemption provisions was to establish a new federal "floor" for the confidentiality of health information.[234] Prior to the Privacy Rule, Congress and HHS found that a patchwork of state law existed; that is, some states had no or very few health information confidentiality protections while other states had robust health information confidentiality protections.[235] Because the patchwork of state health information confidentiality laws failed to provide a consistent and comprehensive legal foundation relating to health information confidentiality, Congress and HHS desired a national health information confidentiality policy with consistent rules.[236]

---

231 45 C.F.R. § 160.203 (2011) ("A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law.").

232 *Id.* § 160.203(b).

233 *Id.* § 160.202 (defining "more stringent").

234 Final HIPAA Privacy Rule, *supra* note 13, at 82,464 ("The rule sets a floor of ground rules for health care providers, health plans, and health care clearinghouses to follow, in order to protect patients and encourage them to seek needed care. The rule seeks to balance the needs of the individual with the needs of the society. It creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve.").

235 *Id.* at 82,466 ("States have, to varying degrees, attempted to enhance confidentiality by establishing laws governing at least some aspects of medical record privacy. This approach, though a step in the right direction, is inadequate. These laws fail to provide a consistent or comprehensive legal foundation of health information privacy. For example, there is considerable variation among the states in the type of information protected and the scope of the protections provided.").

236 *Id.* at 82,466 ("Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections . . . Hence, a national policy with consistent rules is necessary to encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.").

Unlike the topic of health information confidentiality, which prior to the 2003 compliance date for the Privacy Rule did not have a consistent or comprehensive national legal foundation, the topic of attorney-client confidentiality had its start over a century ago. In 1908, the ABA's House of Delegates adopted the ABA Canons of Professional Ethics, including a canon relating to client confidentiality.[237] In 1969 and 1983, the ABA House of Delegates adopted its first Model Code of Professional Responsibility and Model Rules of Professional Conduct, respectively.[238] Both the Model Code and the Model Rules contained rules relating to client confidentiality.[239] Michigan adopted the Model Rules in 1988, and West Virginia, California, and Hawaii followed suit in 1989, 1992, and 1994, respectively.[240] As of today, fifty jurisdictions, including the District of Columbia, have adopted the Model Rules.[241] California is the only state that does not have professional conduct rules that follow the format of the ABA Model Rules.[242]

In summary, one of the reasons for the Privacy Rule's preemption provisions was to establish a new federal "floor" for the confidentiality of health information due to the nonexistence, insufficiency, and/or inconsistency of state law on the topic. In contrast, the ABA through its Model Rules in 1983 (and earlier through its Canons of Professional Ethics in 1908 and its Model Code of Professional Responsibility in 1969) had already established a national, consistent set of rules relating to attorney ethics, including client confidentiality, that nearly every jurisdiction has adopted.

Below, this Article proposes that Congress amend HITECH to give HHS the authority to except certain classes of BAs, including outside counsel, from direct regulation by the Privacy Rule. This proposal has

---

237 *See Model Rules of Professional Conduct: About the Model Rules*, ABA, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (last visited Jan. 29, 2013).

238 *Id.*

239 *See* MODEL CODE OF PROF'L RESPONSIBILITY Canon 4 (1980); MODEL RULES OF PROF'L CONDUCT R. 1.6 (as amended 1983).

240 *See Chronological List of States Adopting Model Rules*, ABA, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/chrono_list_state_adopting_model_rules.html (last visited Jan. 29, 2013).

241 *See Alphabetical List of States Adopting Model Rules*, ABA, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules.html (last visited Jan. 29, 2013).

242 *See Model Rules of Professional Conduct: State Adoption of Model Rules*, ABA, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (last visited Jan. 29, 2013).

its foundation in HHS's decision to except other classes of individuals, institutions, and information from regulation by the Privacy Rule when there exists a national, sufficient, and consistent set of relevant rules. In 2002, for example, HHS exempted from regulation under the Privacy Rule academic institutions that maintained education records that also contain PHI due to the national, sufficient, and consistent confidentiality protections already in place under the federal Family Education Rights and Privacy Act of 1974 (FERPA).[243] HHS reasoned that Congress specifically addressed how academic institutions should protect the confidentiality of education records, including education records that contain PHI, under FERPA and that Congress probably did not intend to amend or preempt FERPA when it enacted HIPAA.[244] HHS further reasoned that it would be unduly burdensome for health care providers employed by academic institutions to have to comply with two different, yet similar, sets of regulations under FERPA and HIPAA.[245]

Similarly, the ABA already specifically addressed how attorneys should maintain the confidentiality of all information relating to a client's representation and that states have responded by enacting their own state rules of professional conduct, almost all of which follow the same format as the ABA's Model Rules. Further, it would be unduly burdensome for attorneys who represent covered entities to have to comply with two different sets of rules; that is, their own state rules of professional conduct and the Privacy Rule, especially when the Privacy Rule is illogical when applied to attorneys.

Instead of challenging or retaining HHS's ability to regulate BAs, Congress should amend HITECH to give HHS the authority to except certain classes of BAs, including outside health care counsel, from direct regulation by the Privacy Rule. There is precedent in other federal health laws for such an exception. When initially enacted in 1989, for example, the federal Stark Law[246] directly regulated physicians who referred Medicare and Medicaid patients to clinical

---

243 Final HIPAA Privacy Rule, *supra* note 13, at 82,483 ("We have excluded education records covered by FERPA . . . from the definition of protected health information. . . . We followed this course because Congress specifically addressed how information in education records should be protected in FERPA. . . . We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA.").

244 *Id.*

245 *Id.*

246 *See* 42 U.S.C. § 1395nn (2006).

laboratories with which the physicians had a financial relationship.[247] Effective in 1995, amendments to the Stark Law expanded the law's application to physicians who referred Medicare and Medicaid patients to entities with which they had a financial relationship for a number of additional designated health services (DHS). In addition to clinical laboratory services, DHS now includes physical therapy, occupational therapy, and outpatient speech-language pathology services; radiology and certain other imaging services; radiation therapy services and supplies; durable medical equipment and supplies; parenteral and enteral nutrients, equipment, and supplies; prosthetics, orthotics, and prosthetic devices and supplies; home health services; outpatient prescription drugs; and inpatient and outpatient hospital services.[248] Given the extremely broad statutory list of DHS for which physicians are prohibited from referring Medicare and Medicaid patients if a financial relationship exists, Congress in the Stark Law gave HHS the authority to except certain relationships from the general referral prohibition.[249] HHS responded by establishing through regulations certain exceptions so that the referral prohibition set forth in the Stark Law was not overly broad and did not prohibit relationships that would not give rise to health care fraud and abuse.[250]

Similarly, Congress should amend HITECH section 13404, codified at 42 U.S.C. § 17934, by adding certain language at the end of subsections (a) and (c). The proposed language would recognize that some classes of BAs: (1) do not have a history, or pattern or practice, of inappropriately using or disclosing their covered entity clients' PHI; (2) are already regulated under other law, such as state law, with respect to their uses and disclosures of their covered entity clients' PHI; and (3) already risk civil, criminal, and/or administrative penalties by agencies with more experience and expertise than HHS in regulating such BAs. The proposed additions to subsection (a) would give HHS the authority to except qualifying classes of BAs from direct regulation by the Privacy Rule and the proposed additions to subsection (c) would except the same qualifying classes of BAs from the additional imposition of civil and criminal penalties by the

---

247 AM. MED. ASS'N, THE STARK LAW RULES OF THE ROAD 2.1 (2011).

248 42 U.S.C. § 1395nn(h)(6).

249 *See id.* § 1395nn(b)(4) (giving HHS the authority to adopt "other permissible exceptions" if the Secretary determines that the excepted relationships do not pose a risk of Medicare or Medicaid Program or patient abuse).

250 *See* 42 C.F.R. §§ 411.350–411.389 (2011).

federal government under the HIPAA statute. The proposed language is italicized and placed at the end of each subsection within 42 U.S.C. § 17934, as follows:

> (a) *Application of contract requirements*. In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subchapter that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity. *The Secretary of the Department of Health and Human Services shall have the authority to except certain classes of business associates from the direct application of this subchapter. The Secretary's authority to grant such exceptions shall be based on evidence showing that the excepted classes: (i) do not have a historical pattern or practice of inappropriately using or disclosing protected health information; (ii) are restricted in using and disclosing protected health information by state or other applicable law; and (iii) are already subject to civil, criminal, and/or administrative penalties for the inappropriate use or disclosure of confidential information by a state or other administrative agency with experience and expertise in regulating the excepted class.*
>
> (c) *Application of civil and criminal penalties*. In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5, 1320d–6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act [42 U.S.C. 1320d et seq.]. *If the Secretary of the Department of Health and Human services excepts a class of business associates from the direct application of this subchapter under subsection (a) of this section, that class of business associates shall also be excepted from the imposition of civil and criminal penalties under this subsection.*[251]

HHS should further amend the Privacy Rule to establish a process through which HHS can implement such exceptions and identify excepted classes of BAs. Specifically, HHS should add the following italicized language to the Privacy Rule at 45 C.F.R. § 164.500(d) establishing the criteria to be used in making exception decisions, as

---

[251] 42 U.S.C. §§ 17934(a), (c) (2011).

well as at 45 C.F.R. § 164.500(e) in order to clarify that state-licensed attorneys have been granted an exception:

> (d) Where provided, *and unless the class to which the business associate belongs has been excepted by the Secretary from direct regulation by this subchapter under subsection (d) of this section*, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.
>
> (e) *The following classes of business associates shall be excepted from direct regulation by this subchapter based on evidence showing that the excepted classes do not have a historical pattern or practice of inappropriately using or disclosing protected health information, are already restricted in using and disclosing protected health information by state or other applicable law, and are already subject to civil, criminal, and/or administrative penalties for the inappropriate use or disclosure of PHI by a state or other administrative agency with experience and expertise in regulating the excepted class: (1) state-licensed attorneys who are required to maintain the confidentiality of client communications and records under state rules of professional conduct and who are subject to disciplinary action by their State Bars for their failure to maintain the confidentiality of client communications; (2) False*

Note that the Secretary may build on the proposed language set forth in 45 C.F.R. § 164.500(e) over time, by adding additional sub-sections at 45 C.F.R. § 164.500(e)(2), (3), (4), etc., to identify additional excepted classes of BAs.

Finally, state bars should consider strengthening the sanctions that may be imposed on licensed attorneys who fail to maintain the confidentiality of client communications and records that contain PHI. In *In re Harman*, remember, the Wisconsin Supreme Court upheld the Wisconsin Board of Attorneys Professional Responsibility's (Board's) decision to impose a six-month suspension of Wisconsin-licensed attorney Harman's license to practice law based on a number of professional failures, including Harman's mishandling of client funds, his representation of a client in the presence of a conflict of interest without obtaining a written consent of the conflict, his knowing disobeyance of an obligation of tribunal rules, his use of information obtained during the representation of a former client to that former client's disadvantage, and his revelation of information relating to the representation of the client without the client's consent.[252] With respect to the last allegation, the Supreme

---

[252] *See In re* Disciplinary Proceedings Against Harman, 628 N.W.2d 351, 354 (Wis. 2001).

Court of Wisconsin held that Harman violated Rule 1.6(a) of the Wisconsin Rules of Professional Conduct for Attorneys when he disclosed the client's PHI, including information stating that the client had a history of drug and alcohol dependence and a history of self-abusive behavior. State agencies such as the Board should be authorized to impose more stringent sanctions when the client communications or records that were inappropriately used or disclosed by the attorney contain PHI. Specifically, the ABA should consider adding a new comment (following the existing nineteen comments that interpret) Rule 1.6 of the Model Rules,[253] as follows:

> Protected Health Information
>
> [20] When using or disclosing client information that contains protected health information, as defined by federal regulation at 45 C.F.R. § 160.103, the lawyer shall recognize the sensitivity of such information. The inappropriate use or disclosure of client information containing protected health information may be considered as an aggravating factor in imposing disciplinary action upon the lawyer.

CONCLUSION

Outside health care counsel frequently obtain medical records, billing records, health insurance claims records, and other records containing individually identifiable health information in the course of representing health industry clients in medical malpractice, licensure, certification, accreditation, fraud and abuse, peer review, and other civil, criminal, and administrative health law matters. This Article is the first to argue that state rules of professional conduct, not federal health information confidentiality regulations, should govern outside health care counsel's use and disclosure of confidential client information.

This Article's proposal—that Congress give HHS the authority to except certain classes of BAs, including outside health care counsel, from direct regulation by the Privacy Rule—is based on several research findings, including the lack of a historical pattern or practice on the part of attorneys in inappropriately using or disclosing PHI, the lack of fit between the health care-related requirements of the Privacy Rule and the legal reasons for which attorneys use and disclose PHI, the presence and effectiveness of state rules of professional conduct that already require attorneys to maintain the confidentiality of client

---

253 *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmts. (2011).

information, the availability of disciplinary action for attorneys who fail to maintain confidentiality, and the experience and expertise of State Bars (and the lack of experience and expertise on HHS's part) in regulating and disciplining attorneys.

Going forward, Congress and HHS should more carefully consider the broad application of health care-related regulations to non-health industry participants. Congress and HHS's desire to protect the confidentiality of PHI from inappropriate uses and disclosures by BAs is laudable. However, the direct regulation of outside health care counsel by the Privacy Rule causes duplication of regulation and disciplinary authority and exacerbates existing conflicts of interest between counsel and their covered entity clients.