NOT SO HIP?: THE EXPANDED BURDENS ON AND CONSEQUENCES TO LAW FIRMS AS BUSINESS ASSOCIATES UNDER HITECH MODIFICATIONS TO HIPAA

Megan Bradshaw[*] *& Benjamin K. Hoover*[**]

ABSTRACT

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") governs the management of protected health information by covered entities (e.g., health care providers) and their business associates. However, the Health Information Technology for Economic and Clinical Health Act ("HITECH"), contained within the American Recovery and Reinvestment Act of 2009 ("ARRA"), drastically alters the scope of HIPAA regulations with regard to business associates, including law firms that routinely handle the protected health information ("PHI") governed by HIPAA. Under the HITECH Act, the definition of "business associate" is expanded, and these entities are treated as "covered" for purposes of the HIPAA security regulations; this increased regulatory burden has important implications for the management of PHI at law firms and the practice of health care law as a whole.

This article details the development of the HIPAA privacy and security regulations applicable to covered

* Associate, Kaufman & Canoles, P.C., Norfolk, Virginia. J.D., 2003, University of Richmond School of Law; B.A., 2000, College of William and Mary.

** J.D. Candidate, 2010, University of Richmond School of Law; B.S., 2007, Pennsylvania State University. The author thanks his friends and family, especially his parents, for their support, and Reneé Reilly, for her boundless love and patience.

entities and business associates in the wake of the HITECH Act, with a focus on the updated regulatory scheme and its impact on law firms, especially those that deal with substantial amounts of PHI in the ordinary course of business. Beyond the development and content of the current HIPAA regulations that impact law firms, this piece addresses the practice implications of these regulations and proposes recommendations for cost-effective and careful handling of PHI from the perspective of business associates and regulators alike.

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was enacted by Congress and signed by President Clinton, ushering in a new era of health insurance regulation, specified medical providers, and private medical information.[1] Under the statutory authority of its provisions, thousands of pages of regulations have been promulgated, influencing the behavior of innumerable covered entities, health care consumers, and business associates, with varying results. In addition to these regulations, entities governed by the provisions of HIPAA have adapted to several amendments of the statute itself, including the recent and significant Health Information Technology for Economic and Clinical Health Act ("HITECH"), contained in the omnibus American Recovery and Reinvestment Act of 2009 ("ARRA").[2]

HIPAA, viewed in the abstract, is overwhelming. Its provisions are codified in scattered sections of the U.S. Code, and its titles govern: (1) access to, portability of, and renewability of health insurance coverage;[3] (2) health care administration and fraud reduction;[4] (3) "[t]ax-related health provisions;"[5] (4) insurance reform provisions;[6] and (5)

1. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of U.S.C.).
2. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, div. A, tit. XIII, 123 Stat. 226 (codified as amended in scattered sections of U.S.C.).
3. HIPAA tit. I.
4. HIPAA tit. II.
5. HIPAA tit. III.
6. HIPAA tit. IV.

employers' revenue offset provisions.[7] While HIPAA's regulatory implications are wide-ranging, this article focuses on the provisions of Title III and the regulations promulgated there under, which govern the management of protected health information ("PHI").

Part II of this article discusses the political background of HIPAA, delving into the factors leading to the statute's enactment, focusing on public opinion, concerns of health care providers, and the political maneuvering required to pass the broadly-encompassing legislation. The examination of the history of HIPAA necessarily discusses the statute's legislative history, providing a theoretical base against which the actual effects of the statute may be measured. Following the examination of HIPAA's background, Part III discusses the enactment of the legislation and its initial reception, as well as the development of regulations under the express authority of HIPAA. This part also provides insight into perceived shortcomings of the legislation through its development. Part IV reviews the rare and important cases involving violations by covered entities decided under pre-HITECH HIPAA and its regulations, demonstrating the consequences facing HIPAA violators under the previous regulatory scheme, as contrasted with the heightened measures of post-HITECH HIPAA. This part additionally provides a vivid illustration of the dormancy of HIPAA enforcement. Part V provides a survey of the HITECH Act amendments to HIPAA as applicable to law firms and other business associates, as well as the pertinent regulations implementing the new statutory provisions. Then, from a prudential prospective, this part explores the regulatory impact of the HITECH amendments to HIPAA and the relevant regulations upon law firms and business associates. This section also examines the financial and practical consequences of post-HITECH HIPAA for lawyers and law firms dealing with substantial amounts of PHI.

II. HIPAA'S HISTORY

A. The Road to HIPAA: Purpose and Enactment

In the last decade of the twentieth century, as the general political climate amplified public concerns over the vulnerability of sensitive medical information, demands for protection of this information correspondingly resounded in editorial pages, talk radio, and ultimately,

7. HIPAA tit. V.

in the halls of Congress. Following political combat over President Clinton's controversial health care plan,[8] which ultimately met defeat,[9] Congress enacted HIPAA with the stated purpose of

> improv[ing] portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance . . . .[10]

Largely due to the intense political controversy surrounding the Clinton health care plan,[11] Congress enacted HIPAA piecemeal through amendments to the Internal Revenue Code[12] and the Social Security Act[13] that became law on August 21, 1996.[14] HIPAA contains two titles designed to effectuate the intent of Congress.[15] The first title addresses health care "access, portability, and renewability,"[16] while the second title governs health care fraud and administration.[17] The HIPAA provisions designed to combat health care fraud and streamline the administration of health care are most relevant because Title II, subtitle

---

8. *See* Robert Pear, *Politics and the Health Care Bill*, NY TIMES, Mar. 24, 1996, at 1. (referencing the Health Security Act, H.R. 3600, 103d Cong. (1994)).
9. *See* Health Security Act, H.R. 3600, 103d Cong. (1994).
10. HIPAA pmbl.
11. As President Clinton stated: "Now, what I tried to do before [enactment of the Clinton health plan] won't work. Maybe we can do it in another way. That's what we've tried to do, a step at a time until eventually we finish this." President Bill Clinton, Remarks to the Service Employees International Union, Washington, D.C. (Sept. 15, 1997).
12. The Internal Revenue Code is found in title 26 of the U.S. Code.
13. 42 U.S.C. §§ 301–1397jj (2006).
14. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of U.S.C.).
15. *See* HIPAA pmbl.
16. HIPAA tit. I. The provisions of Title I generally serve to limit the ways in which health care plans may limit access of consumers to health care, for example, by prohibiting discrimination on the basis of health status or other factors through the use of eligibility rules. *See* HIPAA § 101, 29 U.S.C. § 1182 (2006).
17. HIPAA tit. II.

F supplies the basis for the regulation of entities that handle the health information governed by the Act.[18]

Congress enacted this administrative simplification portion of HIPAA to improve "the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[19] As indicated in the conference report, Congress recognized that some shared uses of personal health information are desirable, and to this end attempted to prevent the curtailment of practices incontrovertibly beneficial to patients and the health care industry.[20] Indeed, HIPAA's billing standardization requirements originated with the efforts of physicians to mandate uniform billing in the 1970s.[21] Thus, from this simple statement of statutory purpose, the majority of regulations impacting law firms and other non-health care business units have ultimately developed, trickling down from regulations governing those entities that primarily develop and process the information of health care consumers. However, the development of these highly relevant regulations was not exactly forthcoming.

B. Development of HIPAA Regulations

While Congress was apparently very concerned with the privacy of health information, it delegated the development of such standards to the Department of Health and Human Services ("HHS") under a mandate requiring specific recommendations for standards governing the privacy of individuals' health information within one year of the enactment of HIPAA.[22] Acting with lamentably poignant foresight, Congress included in HIPAA a provision authorizing the Secretary of HHS ("Secretary") to promulgate privacy regulations in the event that Congress failed to do so within three years of HIPAA's passage.[23]

18. *See* HIPAA §§ 261–264.
19. HIPAA § 261.
20. H.R. REP. NO. 104-736, at 223 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 1990, 2078.
21. Alex L. Bednar, *HIPAA Implications for Attorney-Client Privilege*, 35 ST. MARY'S L.J. 871, 880 (2004).
22. HIPAA § 264(a).
23. HIPAA § 264(c)(1).

Congress did not adopt the recommendations of HHS within its statutorily imposed timeframe.[24] Consequently, the Department initiated the appropriate rulemaking process under section 553 of the Administrative Procedure Act,[25] ultimately issuing the HIPAA privacy and security regulations in 2002 and 2003, respectively.[26] Through this process, the basis of the statutory and regulatory framework to be thrust upon business associates was developed.

III. HIPAA, BUSINESS ASSOCIATES, AND GENERAL STATUTORY AND REGULATORY PROVISIONS

A. General Statutory and Regulatory Provisions

1. Protected Health Information

HIPAA broadly defines "Protected Health Information" ("PHI") as encompassing all "individually identifiable health information [including demographic information] that is:[27] (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium."[28] Therefore, HIPAA's definition of "individually identifiable health information" ("IIHI") facially serves to assuage the concerns of privacy advocates though its expansive and uniform coverage, eliminating the ability of covered entities to elude coverage through the careful selection of information storage media; its coverage is not limited to electronically stored health information.[29]

Such personal health information, to qualify for protection under HIPAA, must originate or be received by a "health care provider, health

24. U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE: HIPAA COMPLIANCE ASSISTANCE 1–2 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.
25. This section provides, among other things, public notice and comment with regard to proposed rules. 5 U.S.C. § 553 (2006).
26. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164 (2009)); 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 (2009)).
27. HIPAA § 262(a), 42 U.S.C. § 1320d(6) (2006); 45 C.F.R. § 160.103 (2009).
28. 45 C.F.R. § 160.103 (2009).
29. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,619 (Dec. 28, 2000).

plan, employer, or health care clearinghouse"[30] and be related to an individual's physical or mental health condition in the past, present, or future.[31] Furthermore, for the information to meet the statutory definition, the individual shall be readily identifiable from the information or there must be a reasonable inference that the information may be used to identify the individual.[32] In utilizing PHI, covered entities must keep disclosure to the "minimum necessary" to accomplish the task at hand.[33]

HIPAA's privacy regulations require covered entities to provide individuals with "adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information."[34] Considering the vast definition of PHI and the penalties imposed upon covered entities for its disclosure,[35] health care providers require patients to sign consents[36] and authorizations[37] for the disclosure of PHI as a matter of routine business practice. This effective waiver of the regulations complicates cost-benefit analysis of the HIPAA privacy regulations, leaving a substantial burden on entities subject to regulation and an absence of benefits ardently sought by consumer privacy advocates during the adoption of HHS's final regulations.[38]

2. Covered Entities

HIPAA initially set forth distinctions between the parties handling the PHI, delineating a special group of health care units known as covered entities.[39] As defined in the regulations, covered entities

30. 42 U.S.C. § 1320d(6)(A) (2006).
31. *Id.* § 1320d(6)(B).
32. *Id.*
33. 45 C.F.R. § 164.502(b) (2009).
34. *Id.* § 164.520(a)(1).
35. *See infra* Part IV.
36. 45 C.F.R. § 164.506(b) (2009).
37. *Id.* § 164.508(a).
38. *See, e.g.*, CTR. FOR DEMOCRACY & TECH., RETHINKING THE ROLE OF CONSENT IN PROTECTING HEALTH INFORMATION PRIVACY 6 (2009) (arguing that consent is inadequate), *available at* www.cdt.org/healthprivacy/20090126Consent.pdf. *Cf.* Jerry LaMartina, *Cost vs. Benefits of HIPAA is Unclear, But Change in Procedures is a Certainty*, KAN. CITY BUS. J., May 17, 2002 (describing possible efficiency gains).
39. 42 U.S.C. § 1320d-1(a) (2006).

governed by HIPAA include health plans, health care clearinghouses, and health care providers.[40] The responsibilities initially imposed on covered entities required each entity to designate a privacy official, whose responsibilities included developing and implementing procedures of the covered entity for compliance with the HIPAA regulations.[41] In addition to the privacy official mandate, the regulations required institutional training of all employees within covered entities and provided guidance regarding the appropriate contours of institutional behavior and handling of PHI and IIHI.[42] Notably, these behavioral regulations prohibit covered entities from requiring waiver of individuals' HIPAA rights as a condition of treatment.[43]

Importantly, these requirements have remained in effect, and have indeed been strengthened as the privacy regulations have evolved in response to political pressure.[44] Business associates were not originally considered covered entities under the HIPAA privacy regulations, but rather were subject to a reduced degree of regulation as partners of covered entities.[45]

B. The Secretary of Health and Human Services Proposes Regulation of "Business Partners"

1. Proposed Regulations

While business associates were not referenced in HIPAA as first enacted, the Secretary proposed the regulation of "business partners"—parties that maintained contractual and other close relationships with covered entities.[46] "Business partners" covered by the proposed regulations included third parties such as administrators, consulting firms, accountants, billing agents, and law firms.[47] The Secretary proposed

40. 45 C.F.R. § 160.103 (2009).
41. *Id.* § 164.530(a)(1)(i).
42. *Id.* § 164.530(b)(1)–(2), (g).
43. *Id.* § 164.530(h).
44. *See infra* Part V.
45. *See* 45 C.F.R. § 164.504(e) (2009).
46. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,933, 59,947 (Nov. 3, 1999). Under the proposed regulations, a business partner was an entity "to whom a covered entity discloses protected health information so that the [entity] can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity." *Id.* at 59,933.
47. *Id.* at 59,947.

that contracts between covered entities and business partners contain "satisfactory assurances" that the PHI transmitted between the covered entity and business partner would be used for the limited purposes of the contract and that its use would conform to the regulations.[48] Finally, HHS proposed that covered entities have the duty to monitor business partners, requiring covered entities to take "reasonable steps to ensure that each business partner complies with the requirements [of the regulations and the contract] with respect to any task or other activity it performs on behalf of the entity . . . ."[49] The enforcement provisions of the proposed regulations named individuals as third party beneficiaries of the business partner contracts; if a business partner disclosed IIHI, the individual whose information was the subject of the breach could sue to terminate the contract.[50]

These proposed regulations prompted backlash from the businesses that would face the new regulatory burden in the form of comments submitted to HHS,[51] testimony before Congress,[52] and pieces published in academic literature.[53] The criticism of the proposed regulations effectively amounted to a protest of increased costs[54] and the failure of HHS to fully combat the law of unintended consequences.[55] The controversy surrounding the original administrative governance of business associates through the HIPAA regulations should have proven instructive for all parties considering the treatment of business associates as covered entities under the HITECH Act amendments to HIPAA.[56]

---

48. *Id.* at 60,054.
49. *Id.*
50. *Id.* at 60,055.
51. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,640 (Dec. 28, 2000).
52. *See, e.g., Examining Medical Records Privacy: Hearing Before the S. Comm. on Health, Educ., Labor and Pensions*, 107th Cong. 42 (2002) (statement of Sam Karp, Chief Info. Officer, Cal. Healthcare Found.).
53. Diane Kutzko et al., *HIPAA in Real Time: Practical Implications of the Federal Privacy Rule*, 51 DRAKE L. REV. 403, 457 (2003).
54. The Secretary's estimate regarding the cost of the new regulations to covered entities was $3.8 billion over five years, but did not account for implementation and administrative costs. 64 Fed. Reg. 59,918, 60,006 (Nov. 3, 1999).
55. *See* Kathleen Dracup & Christopher W. Bryan-Brown, *The Law of Unintended Consequences*, 13 AM. J. CRITICAL CARE 97 (2004).
56. *See infra* Part V.

2. Final Regulations of Business Associates

Following the receipt and consideration of public comment, HHS promulgated final regulations in late 2000, defining "business associates"[57] and their respective obligations to covered entities, as well as their own subcontractors.[58] Under current regulations, "business associates" are persons or organizations that handle a substantial amount of PHI in the performance of functions or services for covered entities involving the disclosure of PHI.[59] Importantly, other covered entities, consultants, accountants, claims processors, and law firms fall within this definition of "business associate."[60] The final regulations regarding contracts[61] between covered entities and business associates: (1) prohibit business associates from disclosing or utilizing PHI beyond the contract terms;[62] (2) require business associates to develop internal guidelines regarding the handling of PHI;[63] (3) mandate the opening of business associate records to HHS and covered entities, upon request;[64] and (4) compel the inclusion of terms assuring that the business associate will comply with the contract and applicable regulations.[65] However, the burden upon covered entities to "take reasonable steps to ensure" compliance with the contract was removed from the final regulations and replaced with an affirmative duty in the instance of known violations.[66] The final regulations also removed the third party beneficiary provision due to the apprehension of HHS regarding the

57. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,475 (Dec. 28, 2000) (codified as amendment at 45 C.F.R. § 160.103 (2009)). The "business partner" terminology was replaced by "business associate" to conform to existing regulations. *See id.*

58. *See id.* at 82,641.

59. 45 C.F.R. § 160.103 (2009).

60. *See id.*

61. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,264 (Aug. 14, 2002) (providing a sample business associate agreement).

62. 45 C.F.R. § 164.504(e)(2)(ii)(A) (2009).

63. *Id.* § 164.504(e)(2)(ii)(B).

64. *Id.* § 164.504(e)(2)(ii)(H).

65. *Id.* § 164.504(e)(2)(i).

66. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,505 (Dec. 28, 2000) (codified as amended at 45 C.F.R. § 164.504(e)(1)(ii) (2009)). Knowledge "of a pattern of activity or practice" constituting a material breach is necessary to give rise to a covered entity's duty to terminate a business associate contract. 45 C.F.R. § 164.504(e)(1)(ii) (2009).

complication of existing third party liability schemes under state law.[67] With regard to the relationship between business associates and their subcontractors, the final regulations imposed the same duties of business associates upon the subordinate parties, forcing these parties to step into the shoes of the business associates when performing "business associate functions."[68]

IV. PENALTIES FOR HIPAA VIOLATIONS AND NOTABLE PRE-HITECH CASES

A. Civil and Criminal Penalties Under HIPAA

In the event that a covered entity failed to comply with HIPAA privacy or security regulations, HIPAA, as originally enacted, provided government units the authority to impose civil and criminal penalties, and such remedies remain viable enforcement mechanisms,[69] even after continued revision.[70] The pre-HITECH Act civil penalty section of HIPAA provided the Secretary with the authority to impose a fine of up to $100 for each civil violation of HIPAA requirements and standards, not to exceed $25,000 for violations of a given "requirement or prohibition" during a single calendar year.[71] The imposition of such fines required that the person against whom the penalty would be assessed had actual or constructive knowledge, through the exercise of "reasonable diligence," about the violation.[72] The Act also excused failure to comply if "due to reasonable cause and not to willful neglect"[73] and if the noncompliance was corrected during a thirty-day period beginning on the first day of actual or constructive knowledge of the violation.[74] Finally, HIPAA, as originally enacted, precluded any civil

67. 65 Fed. Reg. 82,462, 82,506 (Dec. 28, 2000).
68. *Id.* (codified as amended at 45 C.F.R. § 164.504(e)(2)(ii)(D) (2009)).
69. *See* HIPAA § 262(a), 42 U.S.C. §§ 1320d-5, 1320d-6 (2006) (providing civil and criminal penalties).
70. *See infra* Part V; *see also* HITECH Act, Pub. L. No. 111-5, §§ 13401, 13410, 13423, 123 Stat. 226, 260, 271–76, 277 (2009).
71. 42 U.S.C. § 1320d-5(a)(1).
72. *Id.* § 1320d-5(b)(2).
73. *Id.* § 1320d-5(b)(3)(A)(i).
74. *Id.* § 1320d-5(b)(3)(A)(ii). The Act gave the Secretary the authority to extend this period "as determined appropriate" and to supply technical assistance to help the party attain compliance during the period. *Id.* § 1320d-5(b)(3)(B).

penalties for acts criminally punishable under the relevant section of HIPAA.[75] Many of these basic components remain available in the event of civil HIPAA violations; however, the HITECH Act and the interim rules promulgated there under drastically altered the scope of these provisions.[76]

Correspondingly, the criminal provisions served to punish any individual who knowingly misuses a unique health identifier, causes such an identifier to be misused, or obtains or discloses individually identifiable health information.[77] Criminal penalties ranged from a fine of less than $50,000 and/or imprisonment of less than one year, to a fine of less than $250,000 and/or ten years' imprisonment or less if the offense was committed with the intent to obtain economic or personal advantage, or to maliciously harm another.[78]

Despite the public interest in maintaining the privacy of individuals' health care records, Congress did not include a private cause of action in HIPAA, which would have allowed individual recovery against a covered entity that violates the pertinent regulations under the statue.[79] Nevertheless, a number of actions have unsuccessfully attempted to obtain private recovery for alleged HIPAA violations.[80] The statute and regulations do provide some utility for private civil litigants, however;

---

75. *Id.* § 1320d-5(b)(1).

76. *See* HITECH Act, Pub. L. No. 111-5, § 13410, 123 Stat. 226, 271–76 (2009) (codified 42 U.S.C.A. § 1320d-5 (West Supp. 2009)); *infra* Part V.

77. HIPAA § 262(a), 42 U.S.C. § 1320d-6(a) (2006).

78. *Id.* § 1320d-6(b).

79. *E.g.*, Bagent v. Blessing Care Corp., 844 N.E.2d 469, 472 (Ill. App. Ct. 2006), *rev'd on other grounds*, 862 N.E.2d 985 (Ill. 2007).

80. Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006); Smith v. Smith, No. 07-CV-242-JBC, 2007 WL 2332394, at *1–2 (E.D. Ky. Aug. 13, 2007) ("Smith's Complaint alleges that the Defendants obtained his medical records from health care providers under the auspices of [HIPAA] without affording him the opportunity to object to the disclosure. Smith alleges such conduct violated HIPAA and exposes the Defendants to liability under 42 U.S.C. § 1320d-2 . . . ."); Logan v. Dep't of Veterans Affairs, 357 F. Supp. 2d 149, 155 (D.D.C. 2004) (holding that because HIPAA provides HHS the exclusive authority to enforce its provisions, there is no basis to imply a private cause of action); Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004).

violation of HIPAA may be allowed as evidence of other civil causes of action in certain jurisdictions.[81]

B. Covered Entity Violations and Prosecutions

1. HIPAA Criminal Prosecutions

The first criminal prosecution for a HIPAA violation occurred in mid-2004, with charges brought in the Western District of Washington against a phlebotomist who used the medical records of a cancer patient to obtain credit cards.[82] Following a $9,000 spending spree, the defendant was arrested.[83] The charges resulted in a guilty plea and a sixteen-month prison sentence for the defendant, but his employer did not face any civil or criminal liability.[84] Subsequent convictions resulted from a FBI sting operation in Texas[85] and a Florida scheme in which HIPAA-protected information was stolen, transferred, and ultimately used to submit fraudulent Medicare claims.[86] Despite these early successes, criminal prosecutions of HIPAA violations have not since increased in number or frequency; the Department of Justice has received only a few hundred reports of suspected criminal violations from the Office of Civil Rights.[87]

2. Imposition of Civil Penalties

Correspondingly, the imposition of civil penalties under the HIPAA privacy regulations is nonexistent. As of late 2006, no fines were

81. *See, e.g.*, Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006) (invoking HIPAA as evidence of the appropriate standard of care in a negligence action).
82. United States v. Gibson, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. Aug. 19, 2004).
83. *Id.*
84. *See id.*
85. Doreen Z. McQuarrie, *HIPAA Criminal Prosecutions: Few and Far Between*, HEALTH L. PERSP., Feb. 19, 2007, at 3 & n.27, *available at* www.law.uh.edu/healthlaw/perspectives/2007/(DM)HIPAACrimCharges.pdf (citing United States v. Ramirez, No. 7:05CR00708 (S.D. Tex. Aug 30, 2005)).
86. *Id.* at 4 & n.31 (citing United States v. Ferrer, No. 06-60261CR-COHN (S.D. Fla. Sept. 7, 2006)).
87. *Id.* at 1.

imposed for violations of the privacy regulations, and after three years of criticism, no fines have been levied as of early 2009.[88]

C. Business Associate Violations

Under pre-HITECH Act regulation, business associate violations of the HIPAA privacy regulations went largely unrecognized, for reasons unknown.[89] In light of the dearth of apparent business associate violations and the general lack of HIPAA enforcement against covered entities themselves, it is difficult to formulate a sound basis for the expansion of business associate liability through the HITECH Act.

V. HITECH EXPANDS HIPAA BURDENS ON LAW FIRMS

A. Legislative History

The HITECH Act, contained within ARRA, allowed President Obama to keep a promise he made on January 8, 2009 at George Mason University. He promised:

> To improve the quality of our health care while lowering its costs, we will make the immediate investments necessary to ensure that, within five years, all of America's medical records are computerized . . . . This will cut waste, eliminate red tape and reduce the need to repeat expensive medical tests . . . . But it just won't save billions of dollars and thousands of jobs; it will save

88. *See* Elizabeth S. Roop, *Pulling It Together—The HITECH Act & HIPAA*, 21 FOR THE REC. 10 (2009); Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A1; *see also* Maxwell v. Barney, No. 2:06-CV-00840, 2008 WL 1981666, at *6 (D. Utah 2008) ("This complaint alleged that Gold Cross violated HIPAA by providing Knight with a copy of the ambulance ticket. After an initial investigation, HHS declined to pursue prosecution and dismissed the complaint finding that Gold Cross did not violate the HIPAA privacy rule.").

89. Indeed, the authors did not locate any highly publicized cases of breach by business associates. Such cases would have involved breach-of-contract claims by covered entities against their business associates.

> lives by reducing the deadly but preventable medical errors that pervade our health-care system.[90]

Introduced as House Bill 1 by Representative David R. Obey on January 6, 2009, the bill's stated purpose to make "supplemental appropriations for job preservation and creation, infrastructure investment, energy efficiency and science, assistance to the unemployed, and State and local fiscal stabilization, for fiscal year ending September 30, 2009, and for other purposes"[91] would not seem to contemplate a massive change to HIPAA. However, the Act buried a comprehensive alteration within its sweeping legislation, as many entities discovered after the law was signed into effect on February 17, 2009.[92]

The legislature claims that electronic health records are going to "save lives and lower costs."[93] The legislature anticipates that based on federal incentives to adopt electronic health records, a majority of physicians and hospitals will do so, leading to an increased exchange of the electronic health information between entities.[94] The HITECH Act, including the expanded privacy protection to business associates, is billed as necessary to provide for the privacy and security of patients' protected health information given the expanding use of electronic health records.[95] Congress's goal is that all individuals will have electronic health records by 2014.[96]

The Congressional Budget Office ("CBO") stated that adopting health information technology nationwide would shrink total health care spending by "diminishing the number of inappropriate tests and procedures, reducing paperwork and administrative overhead, and decreasing the number of adverse events resulting from medical

---

90. Dan Childs et. al, *President-Elect Urges Electronic Medical Records in 5 Years*, ABCNEWS.COM, Jan. 9, 2009, http://abcnews.go.com/Health/President 44/story?id=6606536&page=1 (last visited Mar. 15, 2010).
91. H.R. 1, 111th Cong. (2009) (enacted); American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, pmbl., 123 Stat. 115.
92. *Id.*
93. Press Release, H. Comm. on Ways and Means, Title IV—Heath Information Technology for Economic and Clinical Health Act (Jan. 16, 2009), *available at* http://waysandmeans.house.gov/media/pdf/110/hit2.pdf.
94. American Recovery and Reinvestment Act of 2009, Joint Explanatory Statement of the Committee of Conference, div. A, subtit. C (2009).
95. *Id.*
96. *Id.*

errors."[97] The CBO predicted that the HITECH Act would increase on-budget deficits by a total of $17.1 billion and the unified budget deficit by an estimated $15.8 billion over the 2009–2019 period.[98] The CBO also predicted that health care costs would decline by approximately 0.3% during the period from 2011–2019.[99] The CBO further observed that health information technology would likely be almost universally adopted over the next twenty-five years even without the government's intervention, which appreciably reduces the impact of decreased spending based on HITECH.[100]

The express purpose of the new law as it relates to business associates is to apply the same security standards and penalties to business associates as are applicable to covered entities.[101] The House Bill also requires HHS to provide annual guidance on technical safeguards, but the Senate Bill did not include this provision.[102] The conference agreement and final public law provide for annual guidance on safeguards.[103]

B. Responsibilities of Law Firms and Attorneys Under Post-HITECH HIPAA

Law firms and lawyers frequently find themselves navigating the well-trod path of HIPAA compliance as business associates. Before HITECH, business associates were liable for HIPAA breaches, but that liability was limited to a breach of contract claim by the relevant covered entity.[104] As pure business associates—business associates who are not also covered entities—law firms were generally only responsible to their covered entities and for harm that was caused by any breach.[105] With the passage of HITECH, the most sweeping health care privacy regulation since HIPAA, lawyers and law firms are faced with a stark new

---

97. Letter from Robert A. Sunshine, Acting Dir., Cong. Budget Office, to the Honorable Charles B. Rangel, Chairman, H. Comm. on Ways and Means 1 (Jan. 21, 2009) (on file with author).
98. *Id.* at 2.
99. *Id.* at 3 & n.3.
100. *Id.* at 3 n.3.
101. American Recovery and Reinvestment Act of 2009, Joint Explanatory Statement of the Committee of Conference, div. A, subtit. D (2009).
102. *Id.*
103. *Id.*
104. *See* 45 C.F.R. § 164.504(e) (2009); *supra* Part III.
105. *See* 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d), (e) (2009). The HIPAA privacy rule previously applied only to covered entities. *See supra* Part III.

HIPAA landscape.[106] As business associates, law firms are now directly responsible for HIPAA compliance.[107] Law firms that receive PHI from their health care clients should realize the significant new responsibilities they have toward the PHI, as well as the new penalties they will face for non-compliance.[108]

1. When is a Law Firm or Attorney a Business Associate?

It does not hurt to begin by reexamining whether a particular law firm is a business associate. If a firm has any health care clients, take a close look at whether it receives any PHI from its clients in the course of representation; if so, the firm will face expanded liability under post-HITECH HIPAA.[109] A law firm's creditors' rights practice or labor and employment practice could be receiving PHI, in addition to the usual suspects in health care litigation.

If a firm is a business associate, now (post-HITECH) is a good time to take a fresh look at where the firm uses PHI. Is PHI involved in limited practice groups or does PHI touch the whole firm? This evaluation can help focus where the efforts on securing information and drafting policies and procedures should be directed. Perhaps most important is an examination of how the firm currently handles and protects PHI. Even without written policies and procedures, firms are, by necessity, doing something to protect PHI already as business associates. Getting a thorough idea of where the firm stands with respect to handling PHI as a business associate should make it easier to fill in the gaps to meet the new requirements.

2. Application of the Security Rule

Business associates must now comply with the administrative, technical, and physical safeguard requirements of the HIPAA Security Rule.[110] Business associates must also implement security policies and

106. Melissa Klein Aguilar, *Coping with Recovery Act's HIPAA Requirements*, COMPLIANCEWEEK.COM, Apr. 7, 2009, http://www.complianceweek.com/article/5350/coping-with-recovery-act-s-hipaa-requirements (last visited Mar. 15, 2010).
107. *See supra* Part III.B.2.
108. *See supra* Part III.B.2; *supra* Part IV.
109. *See supra* Part III.B.2.
110. HITECH Act § 13401(a), 42 U.S.C. § 17931(a) (2006); 45 C.F.R. §§ 164.308, 164.310, 164.312 (2009); *see also supra* Part III.

procedures.[111] Violation of the Security Rule obligations exposes the business associate to both civil and criminal penalties.[112] Compliance with the Security Rule will in all likelihood be the most onerous and costly burden law firm business associates must undertake. There is no distinction made based on the organizational size of the business associate, which means that a large law firm business associate and a solo practitioner business have the same hurdles to clear for compliance with HITECH. While HIPAA allows policies and procedures for safeguarding PHI to take into account the nature and size of activities related to the PHI, simply having a small amount of PHI-related activity or being a small firm is no excuse for failing to establish these mandatory policies and procedures.[113]

3. Administrative Requirements

As previously discussed, the business associate needs a "privacy official."[114] This individual will be responsible for HIPAA policies and procedures.[115] These policies and procedures must be kept by the business associate for six years from the later date of when they were created or were last effective.[116] The business associate must designate an individual responsible for receiving complaints regarding HIPAA compliance[117] and develop a process for receipt of complaints regarding the firm's methods and safeguarding of PHI.[118] Complaints and their dispositions, including sanctions of personnel as appropriate, must be documented by the business associate.[119] While these designees can certainly be individuals within the firm, there are no required qualifications for the designees (e.g., that designees must be current and well versed in the requirements and the firm's policies and procedures).[120] The firm will also have to train members of its firm who deal with PHI on the firm's policies and procedures.[121] Naturally, this

111. HITECH Act § 13401(a), 42 U.S.C. § 17931(a) (2006); 45 C.F.R. § 164.316 (2009).
112. HITECH Act § 13401(b), 42 U.S.C. § 17931(b) (2006).
113. 45 C.F.R. § 164.530(i)(1) (2009).
114. *Id.* § 164.530(a)(1)(i).
115. *Id.*
116. *Id.* § 164.530(j)(2).
117. *Id.* § 164.530(a)(1)(ii).
118. *Id.* § 164.530(d)(1).
119. *Id.* § 164.530(d), (e).
120. *Id.* § 164.530(a)(1)(i) (requiring only an unspecified "privacy official").
121. *Id.* § 164.530(b)(1).

requirement applies to attorneys and paralegals. Also, firms must consider whether clerks, assistants, and internal copy specialists and couriers are exposed to PHI. And, of course, the training of all the aforementioned individuals must be documented.[122] Buried between all of these policies and designees, there is also the requirement to protect PHI from inappropriate use and disclosure with administrative, physical, and technical safeguards.[123]

Law firm business associates without written privacy policies must begin crafting such policies. Assuming the firm is not hiring an outside consultant to handle this albatross (though this option would probably make the firm management's life much easier if it wants to spend the money), it makes sense to form a core group within the firm, probably headed by the designated "privacy official," to determine how the firm is going to safeguard PHI from inappropriate use and disclosure, as well as limiting PHI disclosed "incidentally" in the course of proper use and disclosures.[124]

4. Administrative Safeguards

There is yet another designee: a "security official" whose job is to oversee policies and procedures for administrative safeguards.[125] Firms should embark upon a mandatory risk analysis to evaluate how electronic PHI "confidentiality, integrity, and availability" may be vulnerable and enact ways to reduce the discovered vulnerabilities to an acceptable level.[126] Business associates must establish procedures to regularly review electronic PHI use and access, including tracking access and security "incidents."[127] Further, business associates must sanction personnel who do not comply with the firm's security policies and procedures.[128]

The administrative safeguards focus on access to electronic PHI, specifying that the firm must control access to electronic PHI as central to compliance with these safeguards.[129] Law firms, and their computer systems, are not set up like health care providers' electronic medical

122. *Id.* § 164.530(b)(2)(ii).
123. *Id.* § 164.530(c).
124. *See id.*
125. *Id.* § 164.308(a)(2).
126. *Id.* § 164.308(a)(1)(ii)(A), (B).
127. *Id.* § 164.308(a)(1)(ii)(D).
128. *Id.* § 164.308(a)(1)(ii)(C).
129. *See id.* § 164.308.

records. Thus, controlling and authorizing access is going be a different task for the law firm than it is for the health care provider. Ideally, HHS will provide guidance to business associates on what form compliance with the administrative safeguards can take without drastic intervention or reworking of law firm business associate computer systems. In the meantime, law firms should develop carefully drafted policies and procedures, clarifying that electronic PHI should not be accessed outside of the scope of the business associate agreement. Practices that firms already commonly use, such as locking computers when not in use, certainly do not hurt compliance with the administrative safeguards.

One potential area of concern, that was not as ubiquitous when HIPAA originally took effect, is the handheld PDA that increasing numbers of attorneys use as their lifeline to the office. Is PHI stored on these devices in files and e-mails vulnerable? Until this area is better fleshed out, a policy requiring attorneys to lock their PDAs is a relatively simple way of protecting one potential source of electronic PHI.

5. Physical Safeguards

Compliance with physical safeguards necessitates more policies and procedures. Here, the firm should address physical access to the system that houses electronic PHI, the firm premises, physical access to workstations storing PHI, and the electronic and physical movement of hardware and electronic media containing electronic PHI.[130] Firms should add to the steadily expanding volume of policies and procedures acceptable methods of disposing electronic PHI and reuse electronic media, if desired.[131]

6. Technical Safeguards

The need for more policies and procedures arise in the area of requisite technical safeguards. It is prudent to involve the firm's information technology specialists as available. Technical safeguards deals with allowing access to authorized personnel, including unique identifiers that would allow tracking, for instance, of who is accessing what electronic PHI.[132] Some portions of the technical safeguarding

130. *Id.* § 164.310.
131. *Id.* § 164.310(d)(2)(i), (ii).
132. *Id.* § 164.312 (a).

section are only questionably related to business associates. For example, the law firm business associate is not likely to need emergency access to electronic PHI.[133]

However, a big issue that may be more relevant to the law firm business associate is the requirement for encryption and decryption of electronic PHI.[134] Encryption and decryption will be important when considering the issue of breach notification because the breach notification provisions only apply to PHI that is unsecured.[135] Along the same lines, at least for a technology amateur, the business associate must decide upon a means of preventing unauthorized access to electronic PHI while it is being transmitted electronically.[136]

7. Privacy Rule

The HIPAA Privacy Rule governs use and disclosure of PHI.[137] The Privacy Rule also applies to business associates, but it applies through the obligations set forth in the business associate agreement, as opposed to direct application of the Security Rule.[138] This is a technical distinction because the Privacy Rule also mandates the contents of the business associate agreement, and breach of the business associate agreement now exposes the business associate to civil and criminal penalties expanded from those provided in HIPAA as originally enacted.[139] Business associates can run afoul of the privacy law by improper use and disclosure of PHI or by any use or disclosure of PHI the covered entity improperly disclosed to the business associate.[140] If a business associate knows of a covered entity's pattern of PHI breaches, the business associate could also run afoul of the Privacy Rule by doing nothing.[141]

133. *See id.* § 164.312(a)(2)(ii).
134. *Id.* § 164.312(a)(2)(iv).
135. *See id.*
136. *Id.* § 164.312(e).
137. 45 C.F.R. pts. 160, 164 (2009); *see supra* Part III.
138. HITECH Act § 13404(a), 42 U.S.C. § 17934(a) (2006).
139. *Id.*; 45 C.F.R. § 164.504(e) (2009).
140. HITECH Act § 13404(a), 42 U.S.C. § 17934(a) (2006); 45 C.F.R. § 164.504 (2009).
141. HITECH Act § 13404(b), 42 U.S.C. § 17934(b) (2006); 45 C.F.R. §§ 164.502(e), 164.504(e) (2009).

8. The Business Associate Agreement

The HITECH Act states that the new business associate obligations "shall" be incorporated into business associate agreements.[142] It is not clear whether this means all existing business associate agreements need to be updated to reflect these new obligations, and hopefully there will be forthcoming guidance from HHS. An argument exists that the new obligations are incorporated as a matter of law into business associate agreements as they currently exist. However, the more conservative and better-reasoned interpretation is that revision of business associate agreements is going to be required. At a minimum, all new business associate agreements should reflect the new obligations. Existing business associate agreements for ongoing matters with health care clients should probably also be replaced with a revised version reflecting the business associate's new obligations. Law firms need to evaluate whether they are business associates of any of their health care clients because they may also be assuming responsibility along with the covered entity for ensuring that they enter into a Business Associate Agreement.[143]

9. Show Them the Money: The Penalties

The Centers for Medicare and Medicaid Services ("CMS") enforce the Security Rule,[144] while the Office for Civil Rights, part of HHS, enforces the Privacy Rule.[145] Conventional wisdom predicts that enforcement of all the rules is going to increase, an unsurprising conclusion in light of the current paucity of enforcement actions.[146] Civil monetary penalties assessed are funneled to the Office of Civil Rights for future enforcement of HIPAA.[147]

Violations of HITECH expose business associates to HIPAA's civil and criminal penalties.[148] HITECH's new monetary penalty provisions

142. HITECH Act § 13401(a), 42 U.S.C. § 17931(a) (2006); HITECH Act § 13404(a), 42 U.S.C. § 17934(a) (2006).
143. *See* HITECH Act § 13401(a), 42 U.S.C. § 17931(a) (2006); HITECH Act § 13404(a), 42 U.S.C. § 17934(a) (2006).
144. Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings, 68 Fed. Reg. 18,895 (Apr. 17, 2003) (codified as amended at 45 C.F.R. pt. 160).
145. *Id.*
146. *See supra* Part IV.
147. HITECH Act § 13410, 42 U.S.C. § 17939 (2006).
148. *Id.* § 17939(a)(2).

create different levels of punishment, which are currently in effect.[149] These monetary penalties, limited by calendar year, break down as follows:

1. If the business associate did not know, and should not have reasonably known, that it violated the law:
   a. At least $100 per violation, with identical violations capped at $25,000; and
   b. Maximum $50,000 per violation, with identical violations capped at $1.5 million.[150]
2. Violations due to a "reasonable cause," not willful neglect:
   a. At least $1,000 per violation, with identical violations capped at $100,000; and
   b. Maximum $50,000 per violation, with identical violations capped at $1.5 million.[151]
3. Violations due to "willful neglect" that have been corrected:
   a. At least $10,000 per violation, with identical violations capped at $250,000; and
   b. Maximum $50,000 per violation, with identical violations capped at $1.5 million.[152]
4. Uncorrected violations due to "willful neglect:"
   a. At least $50,000 per violation, with identical violations capped at $1.5 million.[153]

In contrast to previous discretionary compliance reviews of covered entities, the Secretary of HHS now must conduct periodic compliance audits; both covered entities and business associates will be subject to these compliance audits.[154] The design and method of the audits has not been released and will have to be developed by HHS. The Act also empowers state attorney generals with authority to institute civil actions based on violations, including the power to seek injunctions and monetary damages.[155] State attorney generals can seek damages up to $100 per violation, with a maximum of $25,000 for identical violations in a calendar year.[156]

149. HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123 (Oct. 30, 2009) (to be codified 45 C.F.R. pt. 160).
150. HITECH Act § 13410, 42 U.S.C.A. § 1320d-5(a) (West Supp. 2009).
151. *Id.*
152. *Id.*
153. *Id.*
154. HITECH Act § 13411, 42 U.S.C. § 17940 (2006).
155. HITECH Act § 13410, 42 U.S.C.A. § 1320d-5(d) (West. Supp. 2009).
156. *Id.* § 1320d-5(d)(2).

10. Breach Notification

The HITECH Act includes new, daunting breach notifications. The first thing to know is that they only apply to breaches that occur to "unsecured" PHI.[157] PHI that is "secured" in one of the ways specified by HITECH should ease concerns over breach notification. HITECH contemplates "securing" of PHI by either encryption or destruction, the definition of which law firms would be prudent to take note.[158]

C. Help is on the Way

Though it remains to be seen how helpful the assistance forthcoming will be, HHS must designate someone from each regional office to assist business associates into compliance by offering education and guidance.[159] Guidance has started to come out of HHS,[160] though much more would be appreciated by covered entities and business associates alike. Issues, such as what to do with outstanding business associate agreements, would be clarified if additional guidance documents were forthcoming. However, in light of the February 17, 2010 compliance deadline,[161] affected entities must start addressing what they can while waiting on guidance documents.

VI. CONCLUSION

The HITECH modifications to the HIPAA regulatory burden facing business associate lawyers and law firms are appreciable, but should not prove overwhelming with sound decision-making and guidance from HHS. However, the costs of these additional requirements represent another onus upon the legal profession, without any substantial offsetting direct benefit, let alone a larger realized benefit for society as a whole. It seems that a more stringent enforcement pattern will emerge under the post-HITECH HIPAA regulations, but history does not provide a reasonable expectation of this for business associates. In light of expanded administrative requirements and increasing costs, the new regulations will likely prove manageable, but perhaps *Not So Hip* for business associates in the legal profession.

---

157. HITECH Act § 13407, 42 U.S.C. § 17937 (2006); Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740, 42,741 (Aug. 24, 2009).
158. HITECH Act § 13407, 42 U.S.C. § 17937 (2006); 74 Fed. Reg. 42,740, 42,741 (Aug. 24, 2009).
159. HITECH Act § 13403(a), 42 U.S.C. § 17933 (2006).
160. *See* 74 Fed. Reg. 42,740 (Aug. 24, 2009).
161. HITECH Act § 13423, 42 U.S.C. § 17953 (2006).