"SOMETHING WICKED THIS WAY COMES HIPAA AND HER SISTER HITECH" . . . HHS COMPLIANCE AND ENFORCEMENT AND OTHER DEVELOPMENTS IN THE WORLD OF HIPAA

by Brian J. Cohan[*]

* Owner/Founder, Law Offices of Brian J. Cohan, P.C., Long Grove, Illinois; University of Arizona, B.A., cum laude; DePaul University, J.D.

I. INTRODUCTION

Prior to the enactment of the Health Insurance Portability Act of 1996 (HIPAA), there were generally no accepted standards or requirements for protecting personal health care information.[1] The healthcare industry adopted new technologies to pay claims, determine eligibility, and provide and share general health information; thus, the potential for security breaches and risks have increased exponentially.[2] HIPAA and its supporting regulations are the legislature's attempt to provide the privacy and security safeguards necessary for the efficient transmission of this confidential information.[3]

II. STATUTORY AND REGULATORY BACKGROUND

The legislature enacted HIPAA on August 21, 1996.[4] "To improve the efficiency and effectiveness of the health care system, . . . [HIPAA] included Administrative Simplification provisions that required [the Department of Health and Human Services (HHS)] to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security[,]" as well as privacy protections for health information.[5]

The initial HIPAA statute gave Congress a three-year period to implement a rule addressing privacy and security issues related to the exchange, privacy, and security of covered entities' protected healthcare information.[6] Congress failed to act, and the HHS proposed a rule, which it subsequently modified after significant public comment.[7] Congress used these regulations to create the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule), which "establishes . . . national standards for the protection of certain health information."[8]

---

1. *See* U.S. DEP'T. OF HEALTH & HUMAN SERVS., *Security 101 for Covered Entities*, HIPAA SEC. SERIES NO. 1, at 3, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (last modified Mar. 2007) [hereinafter HIPAA SEC. SERIES NO. 1].

2. *See id.*

3. *See id.* at 4.

4. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

5. U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: HIPAA Administrative Simplification Statute and Rules*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html (last visited Mar. 31, 2014).

6. *See* Health Insurance Portability and Accountability Act §§ 261–64.

7. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: Summary of the HIPAA Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Mar. 31, 2014) [hereinafter *Summary of HIPAA Privacy Rule*].

8. *Id.*

Congress also used these regulations to construct the Security Standards for the Protection of Electronic Protected Health Information (Security Rule), which created "a national set of security standards for protecting certain health information that is held or transferred in electronic form."[9] All covered entities must implement this rule by addressing the technical and non-technical safeguards that are necessary to secure individuals' health information.[10]

III. COVERED ENTITIES

The HIPAA Privacy and Security Rules only apply to covered entities and are essentially comprised of any individual or entity that handles individually identifiable health information, or protected health information (PHI), or electronic protected health information (e-PHI).[11] These covered entities include health care plans, health care providers, health care clearinghouses, and by recent amendment, business associates who may come in contact with PHI or e-PHI.[12]

IV. INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

PHI or e-PHI is defined as follows:

> [PHI] is information that is a subset of health information, including demographic information collected from an individual, and:
>
> . . . .
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[13]

V. DE-IDENTIFIED HEALTH INFORMATION

De-identified health information has no restrictions and can be legally de-identified, creating a safe harbor, either by "a formal determination by a qualified expert" or by the proper removal of specified identifiers, including all

---

9. U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: Summary of the HIPAA Security Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (last visited Mar. 31, 2014) [hereinafter *Summary of HIPAA Security Rule*].

10. *See id.*

11. *See* 45 C.F.R. § 160.103 (2012).

12. *See id.*

13. *Id.*

personal data and employer information, as well as relative and next of kin information.[14]

VI. PRIVACY RULE BASIC PRINCIPLE

The major purpose of the Privacy Rule is to define and limit the circumstances in which covered entities may disclose an individual's PHI or e-PHI.[15] "A covered entity . . . may not use or disclose [PHI], except as permitted or required by" the Privacy Rule or as authorized, in writing, by the individual or the individual's personal representative.[16] Under the Privacy Rule, obtaining consent or written permission from individuals is optional for covered entities.[17] The current Privacy Rule protects PHI and is implemented by the Office for Civil Rights (OCR) for a period of fifty years following the patient's death.[18]

Central to the Privacy Rule is the principle of minimum necessary use, disclosure, or request of PHI, which provides that all covered entities must develop and implement policies and procedures to limit uses and disclosures to the minimum amount necessary.[19] When the minimum necessary standard applies, a covered entity may not use, disclose, or request those portions of a medical record that are reasonably needed to accomplish the entity's intended purpose.[20]

Required disclosure only occurs in two instances: first, when individuals or their personal representatives specifically request the disclosure or an accounting of their PHI; and second, when the HHS undertakes a compliance or enforcement investigation.[21]

VII. THE SECURITY RULE

In addition to keeping PHI and e-PHI in compliance with the Privacy Rule, a covered entity must "maintain reasonable and appropriate administrative, technical, and physical safeguards" to prevent intentional or

---

14. U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html (last visited Mar. 31, 2014).

15. *See id.*

16. 45 C.F.R. § 164.502(a).

17. *See id.* § 164.506(b).

18. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: Health Information of Deceased Individuals*, HHS.GOV (Sept. 19, 2013), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/decedents.html.

19. 45 C.F.R. §§ 164.502(b), .514(d).

20. *See id.*; *see also generally* U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: Minimum Necessary Requirement*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html (last modified Apr. 4, 2003) (discussing the use and disclosure of PHI).

21. *See* 45 C.F.R. § 164.502(a)(2).

unintentional use or disclosure of the PHI, as well as to limit the incidental use and disclosure of the PHI.[22]

A. Security Rule General Standards

The United States Code sets out the authority for the HHS to impose standards required under the Security Rule:

> The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for—
> (A) the financial and administrative transactions described in paragraph (2); and
> (B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs, and subject to the requirements under paragraph (5).[23]

These standards govern the affected transactions set forth in § 1320d-2(a)(2) of the United States Code, which includes transactions with respect to the following: claims; enrollment and disenrollment; eligibility questions; payment and remittance advice; premium payments; first report of injury; referral certifications and authorizations; and electronic funds transfer.[24]

Section 1320d-2(a)(4)(A) lays out the following requirements for financial and administrative transactions:

> The standards and associated operating rules adopted by the Secretary shall—
> (i) to the extent feasible and appropriate, enable determination of an individual's eligibility and financial responsibility for a specific services prior to or at the point of care;
> (ii) be comprehensive, requiring minimal augmentation by paper or other communications;
> (iii) provide for timely acknowledgement, response, and status reporting that supports a transparent claims and denial management process (including adjudication and appeals); and
> (iv) describe all data elements (including reason and remark codes) in unambiguous terms, require that such data elements be required or conditioned upon open set values in other fields, and prohibit additional conditions (except where necessary to implement State or Federal law, or to

22. *See* 42 U.S.C. § 1320d-2(d)(2) (2012) (setting out the safeguards under the security standards for health information).

23. *Id.* § 1320d-2(a)(1).

24. *See id.* § 1320d-2(a)(2).

> protect against fraud or abuse [even though compliance can become a costly item, especially for smaller organizations]).[25]

Covered entities should keep in mind that, according to § 164.306 of the Code of Federal Regulations, they must implement reasonable and appropriate security measures, and they must also meet the general requirements set forth in the statute.[26]

The Security Rule permits a covered entity to use any security measure that allows it to reasonably and appropriately fulfill the standards and that is necessary to effectuate any of the technical safeguards set forth in the regulations.[27] The Security Rule also lists the various administrative, physical, technical, and organizational safeguards that must be implemented to obtain compliance.[28]

VIII. ADMINISTRATIVE SAFEGUARDS

The administrative safeguard requirements under the Security Rule are generally set forth in § 164.308(a) of the Code of Federal Regulations and require that covered entities "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[29] The first implementation specification, risk analysis, requires covered entities to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [e-PHI] held."[30] Equally important is the requirement for a risk management implementation plan; this specification requires covered entities to "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)."[31]

Additionally, covered entities must implement a sanction policy, and under that policy, they must "[a]pply appropriate sanctions against workforce members who fail to comply with the[ir] security policies."[32] Another requirement is the information system activity review, which mandates that covered entities "[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports," as well as have assigned security responsibility.[33] The workforce security standard requires covered entities to "[i]mplement policies and procedures to ensure that all members of its workforce have

---

25. *Id.* § 1320d-2(a)(4)(A).
26. *See* 45 C.F.R. § 164.306.
27. *See id.* § 164.306(b).
28. *See id* §§ 164.308, .310, .312, .314.
29. *Id.* § 164.308(a)(1)(i).
30. *Id.* § 164.308(a)(1)(ii)(A).
31. *Id.* § 164.308(a)(1)(ii)(B).
32. *Id.* § 164.308(a)(1)(ii)(C).
33. *Id.* § 164.308(a)(1)(ii)(D); *see also* § 164.308(a)(2).

appropriate access to [e-PHI]" and to promptly terminate those privileges upon termination of employment.[34] The information access management standard requires implementation of "policies and procedures for authorizing access to [e-PHI] that are consistent with the applicable requirements of [the Privacy Rule]," as well as implementation of a security awareness and training program.[35]

IX. PHYSICAL SAFEGUARDS

Physical safeguards are defined as "physical measures, policies, and procedures to protect a covered entity's . . . electronic information systems and related buildings and equipment, from natural and environmental hazards, and from unauthorized intrusion."[36]

A. Facility Access Controls

Covered entities must "[i]mplement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."[37] Additionally, with respect to facility access controls, covered entities must implement a contingency plan for emergency situations, institute a facility security plan, implement access control and validation procedures, regularly make facility security repairs and modifications, including changing of locks and installing new security devices, as well as to provide for general workstation security.[38] Finally, the statute's requirements related to device and media controls—standards for media disposal, media re-use, accountability, and data backup and storage—should not be overlooked.[39]

X. TECHNICAL SAFEGUARDS

The Security Rule does not have specific requirements for the use of any particular type of technology.[40] Rather, the Security Rule allows entities to employ any security measure that is designed to reasonably implement the administrative, physical, technological, and organizational standards.[41] The technical safeguards are generally found in § 164.312 of the Code of Federal Regulations.[42] The first technical safeguard is access control, which requires

34. *Id.* § 164.308(a)(3)(i).
35. *Id.* § 164.308(a)(4)(i); *see also* § 164.308(a)(5)(i).
36. *Id.* § 164.304.
37. *Id.* § 164.310(a)(1).
38. *Id.* § 164.310(a)(2), (c).
39. *Id.* § 164.310(d).
40. *See* HIPAA SEC. SERIES NO. 1, *supra* note 1, at 8.
41. *See id.*
42. *See* 45 C.F.R. § 164.312.

the implementation of unique user identification protocol, emergency access procedures, automatic logoff capabilities, and encryption and decryption mechanisms.[43] Audit control further requires the implementation of "hardware, software, [or] procedural mechanisms that record and examine activity in information systems that contain or use [e-PHI]."[44]

Section 164.312(c)(1) of the Code of Federal Regulations is the integrity standard; this standard requires the implementation of "policies and procedures to protect [e-PHI] from improper alteration or destruction."[45] Covered entities must consider the various risks to the integrity of e-PHI, which has previously been identified in the risk analysis process that the Security Rule mandated.[46] Additional technical safeguards include person or entity authentication and transmission security.[47] Transmission security safeguards require the implementation of "technical security measures to guard against unauthorized access to [e-PHI] that is being transmitted over an electronic communications network."[48]

XI. ORGANIZATIONAL SAFEGUARDS

HIPAA organizational safeguards "requires a covered entity to have contracts or other arrangements with business associates that will have access to the covered entity's [e-PHI]."[49] "In general, a business associate is a person or entity other than a member of the covered entity's workforce that performs functions or activities on the covered entity's behalf, or provides specified services to the covered entity, that involve the use or disclosure of [PHI]."[50]

XII. IMPLEMENTATION SPECIFICATIONS

An implementation specification is classified as either required or addressable.[51] If an implementation specification is classified as addressable, then the covered entity must assess whether the specification is a reasonable and an appropriate safeguard in the entity's particular environment.[52] If, based upon its assessment, the entity chooses not to implement the addressable

---

43. *See id.* § 164.312(a).
44. *Id.* § 164.312(b).
45. *Id.* § 164.312(c)(1).
46. *See supra* note 30 and accompanying text; *see also* U.S. DEP'T. OF HEALTH & HUMAN SERVS., *Security Standards: Technical Safeguards*, HIPAA SEC. SERIES NO. 4, at 8–9, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last modified Mar. 2007).
47. *See* 45 C.F.R. § 164.312(d), (e)(1).
48. *Id.* § 164.312(e)(1).
49. U.S. DEP'T. OF HEALTH & HUMAN SERVS., *Security Standards: Organizational, Policies and Procedures and Documentation Requirements*, HIPAA SEC. SERIES NO. 5, at 2, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf (last modified Mar. 2007).
50. *Id.*
51. *See* 45 C.F.R. § 164.306(d)(1).
52. *See id.* § 164.306(d)(3)(i).

specification, the entity must document the reason, and if reasonable and appropriate, implement an equivalent alternative measure.[53]

Therefore, for each of the addressable implementations, the entity must do at least one of the following:

> (A) Implement the implementation specification if reasonable and appropriate; or
> (B) If implementing the specification is not reasonable and appropriate—
> (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and
> (2) Implement an equivalent alternative measure if reasonable and appropriate.[54]

XIII. SECURITY RULE ELECTRONIC TRANSMISSION REQUIREMENTS

As discussed previously, HIPAA mandated that the HHS adopt standards for the electronic exchange of administrative and financial health care transactions and required the HHS to use standards developed in the private sector, by private sector development organizations.[55] Accordingly, the HHS chose ANSI ASC X12N standards for all transactions, except for retail pharmacy transactions; thus, all covered entities and business associations must use those standards.[56] Failure to comply with the rules and regulations of the standards can result in a fine of up to twenty-five thousand dollars during a given calendar year.[57] Guides for implementing the ASC X12N standards and the retail pharmacy standards are available online.[58]

XIV. THE HITECH ADDITIVE

The legislature further augmented HIPAA's provisions by passing the Health Information Technology for Economic and Clinical Health (HITECH) Act, which it signed into law on February 17, 2009, with the intent to provide a more significant use of health information technology.[59]

> Section 13410(d) of the HITECH Act . . . revised [§] 1176(a) of the Social Security Act . . . by establishing:

---

53. *See id.* § 164.306(d)(3)(ii)(B).

54. *Id.* § 164.306(d)(3)(ii).

55. 42 U.S.C. § 1320d-2(a)(1), (c) (2012).

56. *See Understanding the HIPAA Standard Transactions: The HIPAA Transactions and Code Set Rule*, AM. MED. ASS'N, http://www.ama-assn.org/resources/doc/psa/hipaa-tcs.pdf (2013).

57. *See* 42 U.S.C. § 1320d-5(a)(3)(A).

58. *See* 45 C.F.R. § 162.920(a), (b): *see also Health Care Documentation and Reference*, WASH. PUBL'G CO., http://www.wpc-edi.com (last visited Mar. 31, 2014).

59. *See* Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009).

- Four categories of violations that reflect increasing levels of culpability;
- Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and
- A maximum penalty amount of $1.5 million for all violations of an identical provision.[60]

Maximum criminal sentences can reach up to ten years for willful and egregious conduct, and strict reporting deadlines are also imposed upon health plans and health clearinghouses—by December 31, 2013, they are required to "certify[] that the data and information systems for [the] plan are in compliance with any applicable standards . . . and associated operating rules."[61] "The Secretary [of the HHS] may designate independent, outside entities to certify that a health plan has complied with the requirements under" the United States Code.[62]

The HITECH Act also includes a mandatory breach notification rule that imposes an affirmative duty upon the holder of PHI to notify the HHS if there is a breach of that information, on an immediate basis if the breach involves five hundred or more individuals, or on an annual basis for breaches involving fewer than five hundred individuals.[63]

A. The Enforcer

The HHS enforces the federal standards that govern the privacy of PHI and the federal standards that govern the security of e-PHI.[64] The Secretary of the HHS delegates enforcement responsibility of the Privacy Rule and the Security Rule to the Office of Civil Rights (OCR).[65] The OCR conducts compliance reviews and investigates complaints, and covered entities must cooperate with such reviews and investigations.[66] The HITECH Act also granted state attorney generals concurrent jurisdiction to prosecute money damages and injunctive claims under HIPAA.[67]

---

60. U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: HITECH Act Enforcement Interim Final Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited Mar. 31, 2014); *see also* Health Information Technology for Economic and Clinical Health Act § 13410(d) (current version at 42 U.S.C. § 1320d-5(a)).

61. 42 U.S.C. § 1320d-2(h)(1)(A); *see also id.* § 1320d-6(b)(3).

62. *Id.* § 1320d-2(h)(4).

63. *See* Health Information Technology for Economic and Clinical Health Act § 13402 (current version at 45 C.F.R. §§ 164.400–.414).

64. *See Summary of HIPAA Privacy Rule, supra* note 7; *Summary of HIPAA Security Rule*, *supra* note 9.

65. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: HIPAA Enforcement*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html (last visited Mar. 31, 2014).

66. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: How OCR Enforces the HIPAA Privacy & Security Rules*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html; *see also* 45 C.F.R. §§ 160.306(c), .308, .310(b).

67. *See* Health Information Technology for Economic and Clinical Health Act § 13410(e) (current version at 42 U.S.C. § 1320d-5(d)).

The Secretary of the HHS is authorized to impose, against any covered entity, comprehensive medical plans, which are subject not only to the approval of the Attorney General but also the limitations set forth in the United States Code, including health care plans, health care clearinghouses, or health care providers.[68]

XV. STANDARD FOR ELECTRONIC TRANSMISSION OF E-PHI

Under HIPAA, the HHS adopted standards for the electronic exchange of administrative and financial health care transactions and required, when possible, to use standards that private sector development organizations created.[69] Accordingly, the HHS chose ANSI ASC X12N standards for every exchange of health care information that covered entities and their business associates must use, except for retail pharmacy transactions.[70] HIPAA gives the Secretary of the HHS the power to impose monetary fines for failure to comply with these standards, with a calendar year maximum fine of twenty-five thousand dollars for any one person.[71] The guides for implementing the ASC X12N and the pharmacy standards are available for no cost online.[72]

Standard transactions for Electronic Data Interchange of health care data are generally characterized as one of the following: (a) claims and encounter information; (b) payment and remittance advice; (c) claims status; (d) eligibility, enrollment, and disenrollment; (e) referrals and authorizations; and (f) coordination of benefits and premium payment.[73] Under the provisions of HIPAA, if a covered entity conducts one of the listed transactions electronically, then the entity must use one of the abovementioned, adopted standards—the ASC X12N for covered entities and business associates or the NCPDP for retail pharmacy transactions—and the covered entity must employ the strict code sets assigned by the HHS, with unique identifiers for employers and providers.[74]

XVI. SCORECARD OF HHS ENFORCEMENT

As of March 31, 2014 the "HHS . . . has investigated and resolved over [twenty-two thousand] cases by requiring changes in privacy practices and

---

68. *See* 42 U.S.C. § 1320d-2.

69. *See* CTRS. FOR MEDICARE & MEDICAID SERVS., U.S. DEP'T. OF HEALTH & HUMAN SERVS., *Overview of Electronic Transactions & Code Sets*, HIPAA INFO. SERIES NO. 4, at 1, http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/EducationMaterials/downloads/whateelectronictransactionsandcodesets-4.pdf (last modified May 2003) [hereinafter HIPAA INFO. SERIES NO. 4].

70. *See id.*

71. *See* Brian Kamoie, *HIPAA's Electronic Transactions Rule: Implications for Behavioral Health Providers*, *in* HEALTH POLICY ISSUE BRIEFS, at 11 (Behavioral Health Issue Brief Ser. No. 22, 2002).

72. *See* HIPAA INFO. SERIES NO. 4, *supra* note 69, at 8.

73. *See id.* at 2.

74. *See id.*

other corrective actions by the covered entities."[75] According to the HHS, corrective actions "have resulted in change that is systemic and that affects all the individuals they serve."[76]

The HHS and the OCR did not find violations in over 10,057 cases, and in the remainder of the completed cases—56,595 as of March 31, 2014—the "HHS determined that the complaint did not present an eligible case for enforcement."[77] Of these cases, many involved matters alleging violations prior to compliance dates or violations by entities that failed to meet the organizational requirements set forth in § 164.105 of the Code of Federal Regulations.[78]

The HHS most often investigates the following types of HIPAA-related compliance issues:

1. Impermissible uses and disclosures of [PHI];
2. Lack of safeguards of [PHI];
3. Lack of patient access to their [PHI];
4. Uses or disclosures of more than the minimum necessary [PHI]; and
5. Lack of administrative safeguards of [e-PHI].[79]

"The most common types of covered entities that have been . . . [investigated], in order of frequency[,]" are as follows: "1. Private Practices; 2. General Hospitals; 3. Outpatient Facilities; 4. Health Plans (group health plans and health insurance issuers); and[] 5. Pharmacies."[80]

The HHS enforcement tally may give people a false sense of security, and the evidence suggests that the HHS will normally take a corrective action approach and move forward when infractions and vulnerabilities are *de minimus*.[81] However, when the breaches involve larger vulnerabilities, the HHS is not hesitant to take a swift, and sometimes draconian, action.[82]

XVII. THE HIPAA "SMALL CLAIMS" CASE-THE HOSPICE OF NORTH IDAHO

When the Hospice of North Idaho (HONI) settled its HIPAA security case with the HHS, it was the first settlement related to a data breach that involved

75. U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy: Enforcement Highlights*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights (last modified Apr. 11, 2014).

76. *Id.*

77. *Id.*

78. *See id.*

79. *Id.*

80. *Id.*

81. *See id.*

82. *See, e.g.*, Press Release, U.S. Dep't of Health & Human Servs., Mass. Provider Settles HIPAA Case for 1.5 Million (Sept. 17, 2012), *available at* http://www.hhs.gov/news/press/2012pres/09/20120917a.html [hereinafter Press Release: MEEI].

less than five hundred individuals.[83] Following a familiar theme, the breach resulted from the theft of an unencrypted laptop computer that held the e-PHI of 441 patients.[84] During the investigation, the HHS and the "OCR discovered that HONI had not conducted a risk analysis to safeguard" its patients' e-PHI.[85] Additionally, HONI was lacking policies and procedures, as required by the Security Rule, to address the security of mobile devices.[86] HONI's failure to properly analyze the risks associated with not safeguarding e-PHI, as well as its failure to create appropriate policies and procedures to protect e-PHI stored in, or transmitted by, portable devices, was also troubling to the HHS.[87]

To settle the matter, HONI agreed to pay the HHS fifty thousand dollars, and it also agreed to undertake a corrective action plan (CAP), which included a two-year supervisory period.[88] Leon Rodriguez, the Director of the OCR, commented, "This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information. . . . Encryption is an easy method for making lost information unusable, unreadable[,] and undecipherable."[89] The HHS stressed that covered entities must effectuate a culture of compliance, with additional emphasis on the uses of, as well as the safeguards for, portable electronic devices, devices that are frequently at the center of such data breaches.[90]

XVIII. LOOSE LIPS SINK SHIPS—THE SHASTA REGIONAL MEDICAL CENTER

In January 2012, the Los Angeles Times published an article indicating that two senior executives of the Shasta Regional Medical Center (SRMC) divulged a patient's medical records, as well as the services rendered, without the patient's written authorization, during a meeting with a reporter at a local newspaper.[91] Following the release of this article, the OCR opened a compliance review of SRMC; upon further investigation, the OCR found "that SRMC failed to safeguard the patient's [PHI] from impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate

83. *See* Press Release, U.S. Dep't of Health & Human Servs., HHS Announces First HIPAA Breach Settlement Involving Less Than 500 Patients (Jan. 2, 2013), *available at* http://www.hhs.gov/news/press/2013pres/01/20130102a.html.

84. *See id.*

85. *Id.*

86. *See id.*

87. *See id.*

88. *See id.*

89. *Id.*

90. *See id.*

91. *See* Michael Hiltzik, *Her Case Shows Why Healthcare Privacy Laws Exist*, L.A. TIMES, Jan. 4, 2012, http://articles.latimes.com/2012/jan/04/business/la-fi-hiltzik-20120104.

occasions, without valid written authorization."[92] SRMS shared impermissible information, including information pertaining to "the patient's medical condition, diagnosis[,] and treatment in an email to [its eight hundred member] workforce."[93] Additionally, the OCR found that "SRMC failed to sanction its workforce members for impermissibly disclosing the [protected information] pursuant to its internal sanctions policy."[94]

For its part, SRMC remitted a civil monetary penalty (CMP) of two hundred seventy-five thousand dollars and executed a CAP agreement, which "require[d] SRMC to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members" to ensure that they know how to comply with applicable rules and procedures.[95]

California's regulators also fined Prime Health ninety-five thousand dollars for the privacy breach, and Prime Health is currently being subjected to another HHS investigation, focused upon its coding and its diagnosis of certain medical conditions.[96]

XIX. CMP "LIGHT" AT IDAHO STATE

While the four hundred thousand dollars CMP paid to Idaho State University (ISU) is modest in comparison to other cases, it illustrated some of the heightened exposures presented by the Privacy Rule and the Security Rule with regard to non-covered entities.[97] It also roundly illustrates, as did the SRMC matter, that HHS investigations have a tendency to expand.[98]

In August 2011, the HHS received a HITECH Act notification from ISU regarding a potential breach of unsecured e-PHI.[99] After the OCR commenced an investigation, it concluded the following:

> i. ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012;

---

92. Press Release, U.S. Dep't of Health & Human Servs., HHS Requires Cal. Med. Ctr. To Protect Patients' Right to Privacy (June 13, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/shasta-agreement-press-release.html.

93. *Id.*

94. *Id.*

95. *Id.*

96. *See* Chad Ternune, *Prime Healthcare Settles Federal Patient-Privacy Case for $275,000*, L.A. TIMES, June 11, 2013, http://articles.latimes.com/2013/jun/11/business/la-fi-mo-prime-healthcare-patient-privacy-20130611.

97. *See* Press Release, U.S. Dep't of Health & Human Servs., Idaho State Univ. Settles HIPAA Sec. Case for $400,000 (May 21, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement-press-release.html.html.

98. *See id.*

99. *See* U.S. Dep't of Health & Human Servs., *Resolution Agreement*, at 1, HHS Transaction No. 11-130876 (May 13, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.pdf.

> ii. ISU did not adequately implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and
> iii. ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.[100]

ISU agreed to pay the HHS a CMP of four hundred thousand dollars, and additionally, ISU agreed to enter into a CAP agreement, which required ISU to comply with the following terms:

> A. Hybridization
> 1. ISU shall provide [the] HHS with documentation designating it as a hybrid entity and identifying all of its components that have been designated covered health care components within 30 days of the Effective Date.
> B. Risk Management
> 1. ISU shall provide [the] HHS with its most recent risk management plan that includes specific security measures to reduce the risks and vulnerabilities to a reasonable and appropriate level for all of its covered health care components.
> . . . .
> C. Information System Activity Review
> 1. ISU shall provide [the] HHS with documentation of implementation of its policies and procedures regarding information system activity across all of its covered health care component clinics.
> . . . .
> D. Compliance Gap Analysis
> 1. ISU shall provide documentation of its updated compliance gap analysis activity entitled *Post Incident Risk Assessment*, as specified by [the] HHS, indicating changes in compliance status regarding each Security Rule provision. Such documentation shall include, but is not limited to, a copy of the contingency plan and the documents implementing the contingency plan[,] as well as a listing of all technical safeguards implemented . . . across its covered health care component clinics, within 30 days of the Effective Date.[101]

Therefore, ISU's lawyers will be busy in the foreseeable future.[102]

100. *Id.*
101. *Id.* at 5–6 (alteration to original).
102. *See id.*

XX. THE "WHAT HAPPENED TO THE OLD COPIER HEADACHE"—AFFINITY HEALTH PLAN, INC.

In 2010, a representative of CBS Evening News notified Affinity Health Plan, Inc. that, "as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity" that was equipped with a hard drive containing the e-PHI of Affinity Plan members.[103] In accordance with the requirements of the HITECH Act's Breach Notification Rule, Affinity notified the HHS of the data breach.[104]

Affinity estimated that this particular breach may have affected over 344,000 Affinity patients.[105] The OCR's subsequent investigation confirmed that Affinity illegally disclosed the e-PHI "when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives."[106] Furthermore, the OCR's investigation also indicated "that Affinity failed to incorporate the [e-PHI] stored on photocopier hard drives in its analysis of risks and vulnerabilities[,] as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents."[107] To settle its potential violations, Affinity paid a CMP of $1,215,780.[108]

In addition to the CMP payment, Affinity entered into a CAP Agreement requiring it "to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain[ed] in the possession of the leasing agent[] and to take certain measures to safeguard all" of its e-PHI.[109]

XXI. THE MILLION-DOLLAR LAPTOP

The HHS commenced an investigation of Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (MEEI), after receiving a data breach report that MEEI submitted to its department, in accordance with the HITECH Act's Breach Notification Rule.[110] In its submission, MEEI reported the theft of an unencrypted laptop computer, which contained the e-PHI of MEEI patients, as well as patient prescription information and clinical information.[111]

---

103. Press Release, U.S. Dep't of Health & Human Servs., HHS Settles with Health Plan in Photocopier Breach Case (Aug. 14, 2013), *available at* http://www.hhs.gov/news/press/2013pres/08/20130814a.html.

104. *See id.*

105. *See id.*

106. *Id.*

107. *Id.*

108. *See id.*

109. *Id.* The corrective measures that Affinity was required to undertake to safeguard all of its e-PHI were not specified. *See id.*

110. *See* Press Release: MEEI, *supra* note 82 (indicating that Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. are collectively known as MEEI).

111. *See id.*

Based on its investigation, the OCR concluded as follows:

> MEEI failed to take necessary steps to comply with certain requirements of the Security Rule, such as conducting a thorough analysis of the risk to the confidentiality of [e-PHI] maintained on portable devices[;] implementing security measures sufficient to ensure the confidentiality of [e-PHI] that MEEI created, maintained, and transmitted using portable devices[;] adopting and implementing policies and procedures to restrict access to [e-PHI] to authorized users of portable devices[;] and adopting and implementing policies and procedures to address security incident identification, reporting, and response.[112]

According to the OCR, the "investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the Security Rule."[113]

MEEI paid a $1.5 million CMP to settle the prospective HIPAA violations and agreed to enter into a CAP agreement with the HHS, which required MEEI to review, revise, and maintain policies and procedures to ensure compliance with the Security Rule.[114] Pursuant to the CAP agreement, an independent monitor will conduct assessments of MEEI's compliance with agreement and will render semi-annual reports to the HHS detailing MEEI's compliance over the CAP's three-year period.[115]

Shortly after the settlement between MEEI and the HHS, Leon Rodriguez, the Director of the OCR, made the following comment:

> "In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices[.]" . . . "This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom."[116]

XXII. NORTHERN EXPOSURE—THE ALASKA DHSS

In October 2009, the Alaska Department of Health and Social Services (DHSS) submitted a HITECH Act self-reporting notice to the HHS.[117] The

---

112. *Id.*

113. *Id.*

114. *See* U.S. Dep't of Health & Human Servs., *Resolution Agreement*, at A-3, OCR Complaint No. 10-111355 (Sept. 13, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf.

115. *See id*. at A-6 to A-9 .

116. Press Release: MEEI*, supra* note 82

117. *See* Press Release, U.S. Dep't of Health & Human Servs., Alaska Settles HIPAA Sec. Case for $1,700,000 (June 26, 2012), *available at* http://www.hhs.gov/news/press/2012pres/06/20120626a.html.

notice "indicated that a portable electronic storage device . . . potentially containing [e-PHI] was stolen from the vehicle of a DHSS computer technician on or about" three weeks earlier.[118] In January 2010, the OCR notified the DHSS that it would be conducting an investigation that included on-site visits, interviews of its workforce members, written responses to interrogatories, documentation of policies and procedures, information related to training activities, as well as specific "documentation related to compliance with the Privacy and Security Rules."[119]

During the course of its investigation, the OCR found evidence that the DHSS did not have adequate policies and procedures in place to safeguard its e-PHI.[120] Specifically, the investigation concluded that the DHSS had failed to do the following: (a) conduct a risk analysis of the risks and vulnerabilities, as required by the Security Rule; (b) implement proper risk management measures; (c) complete security training for its employees; (d) implement device and media controls at the DHSS; and (e) address device and media encryption, as set forth in the Security Rule.[121] To settle the matter, the DHSS agreed to pay the HHS a CMP of $1.7 million.[122]

The DHSS also entered into an exhaustive CAP agreement with the HHS, which required the DHSS to develop, review, and amend its policies and procedures to gain compliance with the Security Rule.[123] Under the CAP agreement, the DHSS's policies and procedures were required, at a minimum, to include the following content:

1. Procedure for tracking devices containing e-PHI;
2. Procedure for safeguarding devices containing e-PHI;
3. Procedure for encrypting devices that contain e-PHI;
4. Procedure for disposal and/or re-use of devices that contain e-PHI;
5. Procedure for responding to security incidents; and
6. Procedure for applying sanctions to [workforce] members who violate these policies and procedures.[124]

The CAP provided for extensive monitoring as well as monitoring safeguards.[125] Specifically, the DHSS must ensure that employees receive general Security Rule training, as well as training specifically related to carrying out the provisions of the CAP agreement, and the employees of DHSS

118. U.S. Dep't of Health & Human Servs., *Resolution Agreement*, at 1, OCR Transaction No. 10-106853 (June 25, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf.

119. *Id.*

120. *See id.*

121. *See id.*

122. *See id.* at 2.

123. *See id.* at 5.

124. *Id.* at 6.

125. *See id.* at 7–9.

must certify, in writing, that they have received all required training.[126] DHSS is specifically prohibited from allowing any untrained employees to access its e-PHI.[127]

Due to its apparent concern that the DHSS had minimal, if any, policies or procedures in place, the HHS included in the CAP agreement a mandate that the DHSS conduct an exhaustive "assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by DHSS; and[] DHSS shall implement security measures sufficient to reduce the risks and vulnerabilities identified in the risk analysis."[128]

The CAP also designated an independent monitor to review DHSS' compliance with the CAP.[129] "The [m]onitor must certify in writing that it has expertise in compliance with the Security Rule and is able to perform the reviews . . . in a professionally independent fashion[.]"[130] Within ninety days from the date the HHS approves a monitor's service, the monitor must submit a written plan to the HHS and the DHSS adequately describing the monitor's plan for fulfilling his duties.[131] Furthermore, if the monitor revises the plan, then the monitor must notify the HHS of the revisions within ten days from the date such revisions were made; this affords the HHS a continuing right to comment during the pendency of the CAP.[132] Each quarter, the monitor must prepare a report based upon its reviews, must provide the report to the HHS and to the DHSS, and must immediately notify the HHS and the DHSS if there are any significant violations of the CAP.[133] The HHS can remove the monitor if it believes that the monitor lacks the expertise, independence, or objectivity that the CAP requires.[134] Additionally, if the HHS reasonably believes that the monitor's reports or reviews fail to conform to the CAP's requirements or reasonably believes that the monitor's reports or reviews are inaccurate, then the HHS may conduct its own validation review.[135] The CAP also requires implementation reports and annual reports.[136]

XXIII. "THE WELL POINT/WELL DONE MATTER"

Pursuant to requirements set forth in the HITECH Act's Breach Notification Rule, WellPoint, Inc. submitted a breach report to the HHS in the summer of 2010 "regarding a [potential] breach of certain of its unsecured [e-

126. *See id.* at 6.
127. *See id.* at 7.
128. *Id.* at 7. ("DHSS shall provide its risk analysis and description of risk management measures to HHS within 240 days of the Effective Date for review and approval" of the CAP.).
129. *See id.*
130. *Id.*
131. *See id.*
132. *See id.*
133. *See id.* at 7–8.
134. *See id.* at 8.
135. *See id.*
136. *See id.* at 8–9.

PHI]."[137] Specifically, beginning in October 2009, and for approximately six months thereafter, "WellPoint impermissibly disclosed the [e-PHI], including the names, dates of birth, addresses, Social Security Numbers, telephone numbers[,] and health information, of approximately 612,000 individuals whose [e-PHI] was maintained [on WellPoint's] web-based application database."[138]

The HHS's investigation revealed that WellPoint had not only failed to implement sufficient administrative and technical safeguards, as required under the Security Rule, but had also specifically failed to do the following:

> (1) . . . [A]dequately implement policies and procedures for authorizing access to [e-PHI] maintained in its web-based application database[;]
> (2) . . . [P]erform an adequate technical evaluation in response to a software upgrade [to its information systems;]
> (3) . . . [A]dequately implement technology to verify that a person or entity seeking access to [e-PHI] maintained in its web-based application database is the one claimed.[139]

Curiously absent from the HHS's pronouncement was the lack of any mention of a CAP agreement, which is usually present in less egregious cases.[140] However, to settle the actions stemming from any of the potential violations of the Privacy or Security Rules, WellPoint agreed to a CMP of $1.7 million, which calculates to less than three dollars, per violation, without any onerous, short-leash monitoring.[141] Also somewhat uncharacteristic is the lack of official comment from the Director of OCR.[142]

XXIV. THE CIGNET CASE, OR HOW NOT TO DEAL WITH THE REGULATOR

In October 2009, the OCR notified Cignet Health Center (Cignet) of its proposed imposition of a whopping CMP of over $4.3 million against it for allegedly failing to turn over the medical records of forty-one former Cignet patients, upon their request, and for Cignet's subsequent actions and inactions related to its subsequent dealings with the HHS and the OCR.[143]

---

137. U.S. Dep't of Health & Human Servs., *Resolution Agreement*, at 1, HHS Complaint No. 10-116170 (July 8, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf.

138. *Id.* at 2.

139. *Id.* at 1–2.

140. *See id.* at 2–3.

141. *See id.* at 2.

142. *See* Press Release, U.S. Dep't of Health & Human Servs., WellPoint Pays HHS $1.7 Million for Leaving Info. Accessible Over Internet (July 11, 2013), *available at* http://www.hhs.gov/news/press/2013pres/07/20130711b.html.

143. *See* Notice of Proposed Determination from Georgina C. Verdugo, Dir., Office of Civil Rights, U.S. Dep't of Health & Human Servs., to Daniel E. Austin, Cignet Health Ctr., at 1–2 (Oct. 2009) [hereinafter

In its Notice of Proposed Determination, which set forth the proposed the CMP of $4.3 million, the OCR found that the Cignet ignored the requests of the aforementioned forty-one individuals.[144] In its initial correspondence with Cignet, the "OCR notified Cignet in writing of its investigations . . . . [and] requested a response from Cignet."[145] Cignet ignored this request, as well as several follow-up attempts by the OCR to obtain information from Cignet by telephone and two subsequent letters: one letter from the OCR's Region III Manager and second letter from the Office of General Counsel for HHS.[146]

The OCR requested medical records from Cignet for a group of eleven complaints, giving Cignet a final deadline to provide these records by March 17, 2009; however, again, Cignet failed to respond to the OCR's request and failed to produce any of the documents.[147]

"On June 26, 2009, [the] OCR issued a subpoena *duces tecum* directing Cignet to produce the medical records of the individuals in the first group of [eleven] complaints[.]"[148] Cignet ignored the subpoena, which caused the OCR to inform Cignet that, if it persisted, the OCR would petition the court to enforce the subpoena.[149] Cignet continued to ignore the correspondence.[150]

On February 4, 2010, the "OCR filed a petition to enforce [the] subpoena . . . in the United States District Court for the District of Maryland[.]"[151] The court issued a show cause order and set a hearing for March 29, 2010; however, Cignet failed to appear, respond, or defend its actions.[152] The court entered a default judgment against Cignet and ordered it to produce a complete copy of the medical records for the eleven individuals mentioned in the subpoena.[153] Cignet complied in abundance with the order, delivering fifty-nine boxes to the Department of Justice (DOJ); the boxes not only contained the PHI of the eleven individuals from the subpoena, but they also included the medical records of 4,500 other individuals—the OCR never requested these other individuals' medical records.[154]

The OCR received a second group of sixteen complaints, and shortly thereafter, it established another final deadline, September 17, 2009, for Cignet to produce the requested medical records.[155] Again, Cignet failed to respond.[156]

Notice of Proposed Determination], *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetpenaltynotice.pdf.

144. *See id.*
145. *Id.* at 3.
146. *See id.*
147. *See id.*
148. *Id.*
149. *See id.*
150. *See id.*
151. *Id.*
152. *See id.* at 3–4.
153. *See id.* at 4.
154. *See id.*
155. *See id.* at 3.
156. *See id.*

In a subsequent letter to Cignet, the OCR's Region III Manager informed Cignet "that its investigation . . . indicated that Cignet failed to comply with the Privacy Rule" by refusing to turn over copies of the individuals' medical records, and despite the OCR's numerous attempts to resolve the matter, it was not resolved by informal means.[157] The letter went on to state that, as per § 160.312(a)(3) of the Code of Federal Regulations, the OCR was notifying Cignet of its preliminary findings of noncompliance and that additionally, it was giving Cignet an opportunity to supply any evidence of mitigating factors, pursuant to § 160.408 of the Code of Federal Regulations, or alternatively, any affirmative defenses under § 160.410 of the Code of Federal Regulations—the OCR could consider mitigating factors or affirmative defenses when determining Cignet's CMP under § 160.404.[158] In accordance with § 160.412 of the Code of Federal Regulations, the OCR also gave Cignet an opportunity to "submit written evidence to support a waiver of a CMP for violations that were due to reasonable cause and not due to willful neglect[.]"[159] The letter set forth each of Cignet's acts of noncompliance, as well as the possible CMP corresponding with each act.[160] Once again, Cignet ignored the correspondence.[161] The "OCR obtained the authorization of the Attorney General of the United States prior to issuing [its] Notice of Proposed Determination to impose a CMP."[162]

XXV. BASIS FOR CMP IN CIGNET

Eventually, the OCR determined that Cignet was liable for violating the Privacy Rule, and as a result, would be subject to a CMP; specifically, in its Notice of Proposed Determination, the OCR described Cignet's Privacy Rule violations as follows:

> (1) The OCR found that, under § 164.524 of the Code of Federal Regulations, Cignet failed to provide forty-one individuals timely access to obtain their PHI.[163] The OCR further determined that each denial of access constituted a separate and distinct violation that continued, unabated, until April 7, 2010, when Cignet showed up at the DOJ with fifty-nine boxes full of documents.[164]
>
> (b) The OCR concluded that Cignet not only willfully failed to cooperate with an ongoing investigation pursuant to § 160.310(b) of the Code of Federal Regulations, but also, Cignet willfully continued to be

157. *Id.* at 4.
158. *See id.*
159. *Id.*
160. *See id.*
161. *See id.*
162. *Id.*
163. *See id.* at 5.
164. *See id.*

> uncooperative under April 7, 2010.[165] Such violations were the direct result of "Cignet's willful neglect of its obligation to comply with [§ 160.310(b) of the Code of Federal Regulations]."[166] Section 160.401 of the Code of Federal Regulations defines willful neglect as the "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."[167] The OCR also noted that Cignet failed to submit affirmative defenses or any evidence of mitigating factors as a basis for a waiver of the CMP.[168]

"In determining the amount of the CMP for each violation, [the] OCR . . . considered the . . . factors in accordance with 45 C.F.R. § 160.408."[169] In assessing Cignet's CMP, the OCR considered the following aggravating factors:

> (a) These violations hindered the individuals' ability to obtain continuing health care by delaying their receipt of the [PHI] about them when they sought care from physicians other than those at Cignet. 45 C.F.R. § 160.408(b)(3).
> (b) [The] OCR was forced by Cignet's inaction to issue a subpoena *duces tecum* and to file a petition with the U.S. District Court to obtain copies of the [PHI] of [eleven] of these individuals, who are guaranteed by the Privacy Rule to receive a copy of the [PHI] about them in medical records maintained by a covered entity. 45 C.F.R. § 160.408(f).[170]

The OCR determined that Cignet willfully neglected its Privacy Rule obligation under § 160.310(b) of the Code of Federal Regulations by failing to cooperate with its investigation.[171] As a result of its Privacy Rule violation, the OCR did not waive Cignet's CMP under § 160.412 of the Code of Federal Regulations, "even if the payment of the penalty would be excessive relative to the violation."[172] The OCR determined that Cignet's total CMP for its Privacy Rule violations was $4,351,600, with $1,351,600 of the total CMP amount resulting from Cignet's access violations and the remaining $3 million of the total CMP amount resulting from Cignet's failure to cooperate with the OCR's investigation.[173]

---

165. *See id.*
166. *Id.*
167. 45 C.F.R. § 160.401 (2012).
168. *See* Notice of Proposed Determination, *supra* note 143, at 5.
169. *Id.*
170. *Id.*
171. *See id.* at 6.
172. *Id.*
173. *See id.*

XXVI. RECENT DEVELOPMENTS IN PRIVATE RIGHTS AND HIPAA

It is well established that "HIPAA does not create a private cause of action[.]"[174] However, a recent Indiana case illustrates that, in state courts, HIPAA is still a consideration in private causes of action based upon professional liability and negligence.[175] "On July 26, 2013, a jury in Marion County, Indiana, awarded $1.44 million to a Walgreens customer based on allegations that the customer's pharmacist accessed, reviewed[,] and shared the customer's prescription history with others who then used the information to intimidate and harass the customer."[176] Apparently, the pharmacist's husband previously had romantic affair with the customer, resulting in the birth of a child.[177] When the pharmacist discovered the affair, she allegedly retrieved the customer's protected prescription information and turned it over to her husband, who then utilized the information to intimidate the woman when she demanded he pay his child support obligations.[178]

The customer successfully sued both the pharmacist and Walgreens, and "[a]t trial, [she] argued that even though HIPAA did not create a private cause of action, it still defined the standard of care for the pharmacist's duty of confidentiality and privacy to [her PHI]."[179] Furthermore, the plaintiff argued that, since the pharmacist's actions violated the Privacy Rule, the pharmacist had breached the applicable standard of care.[180] Finally, "because the pharmacist had acted within the scope of her employment, [the] plaintiff argued that Walgreens" should also be held liable under the principle of respondeat superior.[181]

XXVII. CONCLUSION

HIPAA, its Privacy Rule, and its Security Rule are self-proclaimed, scalable standards, and judging from the proliferation of electronic devices that store and transmit PHI, these standards will have to be flexible.[182] In counseling covered entities, emphasis is warranted on the risk analysis and the risk management standards found in the Security Rule.[183] Only through conducting a meaningful risk analysis, and implementing steps based upon that

---

174. Cory J. Fox, *HIPAA Violation Results in $1.44M Jury Verdict Against Walgreens, Pharmacist*, BAKERHOSTETLER (August 14, 2013), http://www.bakerlaw.com/health-law-update-august-22-2013#HIPAA (last visited Dec. 19, 2013)

175. *See id.*

176. *Id.*

177. *See id.*

178. *See id.*

179. *Id.*

180. *See id.*

181. *Id.*

182. *See* 45 C.F.R. §§ 160.400–.414 (2012).

183. *See* discussion *supra* Parts VIII, X.

analysis, will the entity have any type of justification for which it can base its HIPAA compliance activities.[184]

If the HHS calls companion state regulators or private plaintiffs into task, the failure to conduct these basic, foundational responsibilities leaves clients open to significant fines and awards.[185] Therefore, either healthcare entities and state healthcare agencies are oblivious to the potential consequences for failing to follow HIPAA's rules and regulations, which does not provide any comfort, or the HHS is determined to enforce HIPAA's rules and regulations in an aggressive, but perhaps inconsistent, manner.[186]

184. *See id.*
185. *See e.g.*, Parts XVII–XXVI.
186. *See id.*