Loyola University Chicago Law Journal

Volume 46
Issue 1 *Fall 2014*

Article 5

2014

Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment

Roger Hsieh
Clerk for Hon. John Z. Lee

Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment

*Roger Hsieh**

Electronic medical records ("EMRs") have helped healthcare organizations improve patient care, but EMRs are susceptible to exposing the confidentiality of patients' medical records to identity thieves and members of the general public. The federal enforcement of patient privacy law—notably the Health Insurance Portability and Accountability Act ("HIPAA"), which was designed to deter and punish breaches of patient privacy—has failed to keep pace with new privacy risks posed by healthcare technology. Although federal legislation now allows state Attorneys General to file suit under HIPAA, for reasons explained in this Article, they too will not enforce HIPAA effectively.

Because institutional enforcement of HIPAA does not adequately protect patient privacy in a digital healthcare environment, this Article proposes a multifaceted solution. In doing so, this Article contributes a framework for categorizing different types of patient privacy breaches, which demonstrates that improving HIPAA enforcement and strengthening patient privacy protections will require different types of solutions depending on the type of breach.

---

* Roger Hsieh received his B.A. from Northwestern University and his J.D. from UCLA Law School. The author clerked for the Honorable John Z. Lee, and prior to law school, the author implemented electronic medical records. I would like to thank Lisa Gillette, Andrew Peterson, Dr. Nick Pytel, Dr. R. Andrew Rowland, Annette Trikoon, my family, and the *Loyola University Chicago Law Journal* for their feedback and support. I would especially like to thank Allison Hoffman for her comments and guidance.

INTRODUCTION

Medical records are private for good reason. In the wrong hands, a patient's social security number; insurance information; list of medications; and history of mental illnesses, sexually transmitted diseases, or other diagnoses could be used for identity theft or to embarrass, harass, or discriminate against the patient. Although private medical information should not be made widely available on a public website, 20,000 patients who visited the Stanford University Emergency

Room in 2009 had their names, account numbers, billing charges, and diagnoses codes (including emergency psychiatric care) published online.[1] Such a breach of medical privacy may cause patients to be skeptical of receiving care, and in some instances, to forego medical care altogether.[2]

Stanford University Medical Center and many other healthcare institutions across the country have implemented Electronic Medical Records ("EMRs"). Although EMRs provide numerous benefits to healthcare providers and patients,[3] an increased adoption of EMRs may help facilitate patient privacy breaches. For instance, an employee with prying eyes ten floors above a patient in the emergency room cannot immediately access the patient's paper chart, but an EMR bridges the physical barrier. Using EMRs, unauthorized employees can (and do) view medical records of celebrities, co-workers, and other patients.[4] EMRs are also susceptible to mass breaches of patient privacy; thieves have stolen millions of medical records containing sensitive personal and financial information.[5]

To protect the privacy of medical records, Congress passed the Health Insurance Portability and Accountability Act ("HIPAA") Privacy

---

1. *See infra* Part I.B.

2. *See* FAIRWARNING, HOW PRIVACY CONSIDERATIONS DRIVE PATIENT DECISIONS AND IMPACT PATIENT CARE OUTCOMES 5 (Sept. 13, 2011) [hereinafter PRIVACY CONSIDERATIONS], *available at* http://www.fairwarning.com/documents/2011-WHITEPAPER-US-PATIENT-SURVEY.pdf (finding 60% of patients no longer sought care from medical providers following a breach of their medical records).

3. *See, e.g.*, Ariele Yaffee, Note, *Financing the Pulp to Digital Phenomenon*, 7 J. HEALTH & BIOMED. L. 325, 334–36 (2011) (describing some benefits of EMRs including: allowing clinicians to access patient charts from anywhere in a hospital, reminding providers of patient allergies and drug interactions, reducing medical errors, and potentially helping save hundreds of thousands of lives by improving disease prevention and management).

4. *E.g.*, *UCLA Hospital to Pay $865,500 in Latest HIPAA Privacy Settlement*, THOMPSON'S HR COMPLIANCE EXPERT (Sept. 1, 2011, 12:00 PM), *available at* http://hr.complianceexpert.com/ucla-hospital-to-pay-865-500-in-latest-hipaa-privacy-settlement-1.57851 (describing when unauthorized University of California at Los Angeles Health System employees repeatedly accessed electronic patient records between 2005 and 2008, and when a researcher improperly accessed the records of co-workers and celebrities).

5. *See, e.g.*, *Health Information Privacy: Breaches Affecting 500 or More Individuals*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Sept. 26, 2014) (documenting 1129 breaches through July 2014 affecting over 38 million patients.) These figures were calculated by first clicking on the "CVS format" link found on the webpage provided. The number of breaches was calculated by the total number of covered entities in Column A (Name of Covered Entity). The number of patients affected was calculated by adding the numbers in Column D (Individuals Affected).

and Security Rules.[6] The HIPAA Privacy Rule empowers the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") to penalize the unauthorized disclosure of "protected health information" ("PHI") and the Security Rule establishes standards to protect electronic PHI.[7] OCR's enforcement of HIPAA in an increasingly digital environment,[8] however, does not properly protect patient privacy.[9] Although the 2009 Health Information Technology for Economic and Clinical Health ("HITECH") Act expanded the enforcement of HIPAA from the OCR to include State Attorneys General ("AGs"),[10] only a few AGs have filed suit under HIPAA since 2009.[11] This Article provides an original analysis explaining why AGs will not enforce HIPAA and why the HIPAA Privacy and Security Rules will remain without strong institutional enforcement.

Given the widespread adoption of EMRs and the challenges in enforcing HIPAA,[12] I propose a new framework for analyzing patient privacy breaches. I first draw distinctions between willful, negligent, and non-negligent patient privacy breaches. These distinctions provide a framework for analyzing a range of solutions to better protect patient privacy. Next, I propose that establishing partnerships between state

---

6. 42 U.S.C. §§ 1320d-2, 1320d-6 (2012).

7. *See infra* text accompanying note 52 (defining PHI). The HIPAA Privacy Rule regulates the use and disclosure of PHI held by "covered entities," limits the disclosure of PHI, and provides civil and criminal penalties for patient privacy breaches. "Covered Entities" include health plans and heath care providers. DEP'T OF HEALTH & HUMAN SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 2–4 (2003), [hereinafter OCR PRIVACY BRIEF] *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. The HIPAA Security Rule requires technical, administrative, and physical safeguards to protect the confidentiality of electronic PHI. *See infra* notes 59–61 and accompanying text.

8. Prompted by government funding and in an effort to improve patient care, healthcare institutions across the country are spending billions of dollars implementing EMRs. *See infra* Part I.A.

9. *See infra* Part I.C.

10. Health Information Technology for Economic and Clinical Health Act § 13410(d), 42 U.S.C. § 1320d-5 (2012). The HITECH Act aimed "to promote the adoption and meaningful use of health information technology" and address "the privacy and security concerns associated with the electronic transmission of health information." HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56,123, 56,124 (Oct. 30, 2009) (codified at 45 C.F.R. § 160 (2013)). HHS issued a notice of proposed rulemaking and stated that giving AGs power to file suit under HIPAA was "designed to strengthen and expand HIPAA's enforcement provisions." Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,869 (July 14, 2010) (codified at 45 C.F.R. §§ 160, 164 (2013)).

11. *See infra* Part II.A (describing four AGs who have filed suit under HIPAA).

12. *See infra* Part I.C.

health agencies and AGs, and considering limited private rights of action, will provide stronger institutional enforcement of HIPAA. Additionally, requiring the encryption of patient data and conducting more HIPAA audits without notice will better protect patients from all three types of privacy breaches.

In Part I, I discuss the prevalence of EMRs, related privacy concerns, and the current state of enforcement of the HIPAA Privacy and Security Rules by OCR. In Part II, I analyze four factors that explain why AGs are unlikely to exercise their HIPAA enforcement powers, including: (1) the lack of time and resources among AGs; (2) the low number of patient privacy complaints received by AGs compared to other areas of consumer protection; (3) the availability of other state law remedies to address patient privacy breaches; and (4) the political nature of the AG position. Finally, in Part III, I establish a framework for analyzing different types of breaches and propose a multifaceted solution for protecting patient privacy and enforcing HIPAA in a digital healthcare environment.

I. ELECTRONIC MEDICAL RECORDS (EMRS): BENEFITS AND PATIENT PRIVACY CONCERNS

A. Benefits and Federal Funding for EMRs

Although EMRs provide additional opportunities for patient privacy breaches, healthcare organizations continue to implement EMRs, given the potential benefits for their patients.[13] EMRs can reduce medical errors from transcription, provide correct dosing for medications, alert providers to adverse drug interactions and allergies, and provide consulting physicians with real time lab results and progress notes to help better care for patients.[14] In addition, EMRs can assist with data collection for research,[15] help providers better manage their patients' long-term chronic diseases,[16] and reduce infant mortality rates.[17]

13. *See infra* note 31 and accompanying text.

14. *See* Yaffee, *supra* note 3, at 333–37.

15. *See, e.g.*, Editorial, *Health Care is Next Frontier for Big Data*, WALL ST. J., Jan. 19, 2012, http://online.wsj.com/article/SB10001424052970204468004577169073508073892.html (describing how "the ability to collect, process and interpret massive amounts of information" in health care gives researchers the ability to analyze information "across time" and "begin the process of pattern recognition").

16. Richard Hillestad et al., *Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 HEALTH AFF. 1103, 1112–13 (2005).

17. *See* Amalia R. Miller & Catherine E. Tucker, *Can Health Care Information Technology*

Moreover, healthcare organizations with hospitals across the country can share patient data with member organizations using EMRs, allowing better care for patients traveling out of state.[18]

Implementing an EMR, however, is usually a time-intensive and costly process. For example, Kaiser Permanente signed a contract to implement an integrated EMR system in 2003.[19] Kaiser finished implementing its EMR system[20] in 36 hospitals and 431 medical offices seven years later[21] and estimates that it will spend a total of $4 billion on the project.[22] The costs of installing EMRs in smaller physician practices can also be significant compared to the size of the practice.[23] These high costs can deter healthcare organizations from implementing an EMR system, and physicians are often less productive after transitioning to an EMR because adjusting to the new computerized system takes time.[24]

To encourage providers and healthcare organizations to implement EMRs, the federal government proposed incentive payments of $19.2 billion through the HITECH Act of the American Recovery and

---

Save Babies?, 119 J. POL. ECON. 289, 290 (2011) (finding that a 10% increase in basic EMR adoption would help save the lives of sixteen babies for every 100,000 births).

18. *E.g.*, Yaffee, *supra* note 3, at 334.

19. Joe Manning, *Madison-Based Firm Wins Records Contract*, MILWAUKEE J. SENTINEL, Feb. 5, 2003, at 1D. In 2003, Kaiser, the country's largest non-profit Health Maintenance Organization, estimated that it would spend $1.8 billion to implement an integrated EMR system. *Id.* at 3D.

20. An EMR refers to a patient's individual electronic medical record. An EMR system, on the other hand, refers to an institution's computerized system, which employees can use to complete tasks such as viewing patient records, scheduling appointments, placing orders, prescribing medication, and billing.

21. Bernie Monegain, *Kaiser KP HealthConnect Rollout Done*, HEALTHCAREIT NEWS, Mar. 29, 2010, at 1, http://www.healthcareitnews.com/news/kaiser-kp-healthconnect-rollout-done.

22. Milt Freudenheim, *Digitizing Health Records, Before it was Cool*, N.Y. TIMES, Jan. 15, 2012, at BU1, http://www.nytimes.com/2012/01/15/business/epic-systems-digitizing-health-records-before-it-was-cool.html?_r=1&pagewanted=all. The $4 billion implementation figure includes costs for software, hardware, and training employees on the use of the electronic system. *Id.*

23. *See* Yaffee, *supra* note 3, at 351 ("The average physician earns between $100,000 and $200,000 annually, and the expense of an EMR system often exceeds $30,000 per physician, making the imposed costs on small practices high."); *see also* Paul D. Smith, *Implementing an EMR System: One Clinic's Experience*, FAM. PRAC. MGMT., May 2003, at 37, 42, http://www.aafp.org/fpm/2003/0500/p37.html (estimating the costs of implementing an EMR at a family medical clinic with six part-time physicians and six resident physicians was between $220,800 and $260,800).

24. *E.g.*, Paul Roemer, *What Does Lost EHR Productivity Cost?*, HEALTHCARE IT STRATEGY (Oct. 25, 2011), http://healthcareitstrategy.com/2011/10/25/what-does-lost-ehr-productivity-cost/.

Reinvestment Act of 2009.[25] The HITECH Act aims to promote EMR adoption through a carrot and stick approach: offering financial incentives to providers who demonstrate "meaningful use"[26] of a certified EMR beginning in 2011,[27] and penalizing providers who do not adopt an EMR by 2015 by withholding Medicare payments.[28]

By May 2013, over half of all eligible providers and approximately 80% of eligible hospitals received HITECH incentive payments for "adopting, implementing, upgrading, or meaningfully using an [EMR]."[29] As of January 2014, eligible hospitals and providers received over $20.9 billion in EMR incentive payments.[30] Given the money invested in implementing EMRs, increased use of EMRs,[31] and potential withholding of Medicare dollars[32] for failing to adopt EMRs, EMRs will continue to play an important role in modern health care.

---

25. Yaffee, *supra* note 3, at 356 n.146.

26. For a list of "meaningful use" requirements, see *2014 Definition Stage 1 of Meaningful Use*, CTR. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html (last updated July 18, 2014, 1:00 PM).

27. Providers may receive up to $44,000 in Medicare subsidies over a five-year period and up to $63,750 in Medicaid subsidies over a six-year period. Early implementers of EMRs will receive the maximum payments. *See The Official Web Site for the Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs*, CTR. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/EHRIncentivePrograms/35_Basics.asp (last updated June 19, 2014, 9:08 AM).

28. Providers who do not adopt an EMR by 2015 will have 1% of Medicare payments withheld and up to 3% withheld if an EMR is not adopted by 2017. ATHENAHEALTH, A SUMMARY OF THE HITECH ACT: WHITEPAPER 3 (Mar. 2009), *available at* http://www.athenahealth.com/_doc/pdf/HITECH_Fact_Sheet_Whitepaper.pdf.

29. Press Release, Dep't Health & Human Servs., Doctors and Hospitals' Use of Health IT More Than Doubles Since 2012 (May 22, 2013), *available at* http://www.hhs.gov/news/press/2013pres/05/20130522a.html.

30. CTR. FOR MEDICARE & MEDICAID SERVS., EHR INCENTIVE PROGRAM (Jan. 2014), *available at* http://cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/January2014_SummaryReport.pdf. Including payments made in 2014, CMS has paid over $22.5 billion in incentive payments, more than the total amount estimated to be paid through 2021. *EHR Incentive Program Exceeds $22.5 Billion Payout Estimate*, HEALTHDATA MGMT., http://www.healthdatamanagement.com/news/EHR-incentives-exceed-estimates-47415-1.html (last visited Sept. 26, 2014).

31. In 2013, 78% of office-based physicians used an EMR, up from 18% in 2001. Chun-Ju Hsiao & Esther Hing, *Use and Characteristics of Electronic Health Record Systems Among Office-Based Physician Practices: United States, 2001–2013*, 143 NAT'L CTR. FOR HEALTH STATS., Jan. 2014, at 1, 1, *available at* http://www.cdc.gov/nchs/data/databriefs/db143.pdf.

32. Medicare spending totaled $524 billion in 2010, comprising 15.1% of the Federal Budget, and is projected to grow to $949 billion in 2020. LISA POTETZ ET AL., MEDICARE SPENDING AND FINANCING: A PRIMER 1 ex.1 (Feb. 2011), *available at* http://www.kff.org/medicare/upload/7731-03.pdf.

B. Patient Privacy Issues with EMRs

Although widespread EMR adoption will bring numerous benefits to healthcare providers and their patients, EMRs will also increase risks to patient privacy. Some individuals may intentionally use an EMR to gain unauthorized access to a patient's medical record. While a traditional medical record was often confined to a hard copy of the patient's chart,[33] an employee may access patient data using almost any computer in a hospital with an EMR system.[34] Once logged into an EMR system, an unauthorized employee can view a patient's medical record with the click of a button.[35] For example, UCLA Medical Center employees accessed Britney Spears's medical record through an EMR when she gave birth at the hospital in 2005 and during her hospitalization in the UCLA psychiatric unit in 2008.[36] As a result of the breach of Spears's medical records, UCLA Medical Center fired at least thirteen individuals.[37]

Celebrity medical records are not the only targets of prying eyes. Inquisitive employees may be able to view the medical records of strangers, friends, or an estranged spouse.[38] Healthcare organizations can attempt to deter unauthorized access to patient records through audit trails and strict disciplinary policies,[39] but EMRs continue to present

---

33. *See* Richard Pollack, *Computerized Patient Record Cuts Redundant Documentation, Improves Charting*, 18 HEALTH MGMT. TECH. 29, 29 (Aug. 1997) (explaining that a paper chart "can only be handled by one person at a time, in one location").

34. *See, e.g.*, *Benefits of the EMR at Mayo*, MAYO CLINIC, http://www.mayoclinic.org/about-mayo-clinic/electronic-medical-record/benefits (last visited Sept. 26, 2014) ("Multiple care providers, in different locations, can simultaneously view a patient's medical record on their computers . . . .").

35. Once logged into an EMR, clinical staff can often look at records of patients throughout the hospital system, including those patients outside of their care or even unit. *See* Yaffee, *supra* note 3, at 343 (footnote omitted) (noting that "recent security breaches at hospitals have led to a myriad of stolen identities (roughly 250,000 to 500,000 per year), fraudulent activities, and invasion of patient privacy at various levels").

36. Charles Ornstein, *Hospital to Punish Snooping on Spears*, L.A. TIMES, Mar. 15, 2008, at A.1, http://articles.latimes.com/2008/mar/15/local/me-britney15.

37. *Id.*

38. Dr. Mark Schleiss, a researcher at the University of Minnesota, used an EMR to access his estranged-wife's and daughters' medical records multiple times. Dr. Schleiss used the EMR to find upcoming appointments, to which he showed up uninvited. Lora Pabst, *Estranged from Family, Doctor Snoops in Records*, STAR TRIB., July 13, 2010, http://www.startribune.com/investigators/98286509.html.

39. The HIPAA Security Rule sets forth guidelines in an effort to prevent these types of individual breaches by requiring hospitals to take certain measures to protect patient data. *See infra* Part I.C. This Article will address possible solutions to deter breaches of this type. *See*

greater patient privacy risks than those found when documenting on paper charts.

In addition to compromising the privacy of isolated individuals, EMRs can also facilitate wide-scale breaches of patient privacy.[40] For example, a thief broke a window at Sutter Medical Foundation and stole a computer containing the medical information of more than 4 million patients in 2011.[41] The data on the computer was not encrypted[42] and contained the personal information—including dates of birth, medical record numbers, addresses, and health insurance plans—of about 3.3 million patients.[43] The medical diagnoses and procedures of almost 1 million patients were also stored on the computer.[44]

While some individuals may intentionally use an EMR to gain unauthorized access to a patient's medical record, carelessness and oversight by those in the healthcare industry can also compromise patient privacy. As mentioned in the Introduction, sensitive information from the medical records of thousands of patients who visited the Stanford University Emergency Department was posted on a public website that allows students to solicit help with their homework.[45] The patient data was stored in a spreadsheet, which made its way to a billing contractor, and then appeared on the website studentoffortune.com in response to a question about creating a bar graph.[46] The spreadsheet included information regarding emergency psychiatric care visits and was available online for nearly one year.[47]

The privacy breaches described above can lead to the exposure of

---

infra Part III.

40. The HIPAA Privacy Rule sets forth guidelines in an effort to deter wide-scale privacy breaches. *See infra* Part I.C. While EMRs can facilitate wide-scale privacy breaches, not all wide-scale privacy breaches are facilitated by EMRs. *See infra* note 51 and accompanying text.

41. Don Thompson & Marcus Wohlsen, *Theft of Data on 4M Patients Part of Wider Problem*, ASSOCIATED PRESS (Nov. 17, 2011), *available at* http://www.boston.com/business/technology/articles/2011/11/17/theft_of_data_on_4m_patients_part_of_wider_problem/.

42. The HIPAA Security Rule does not require healthcare institutions to encrypt patient data. *See* Technical Safeguards, 45 C.F.R. § 164.312(a)(2)(iv) (2013) (listing encryption and decryption of "protected health information" as "addressable" rather than "required"). Requiring encryption of protected health information would better protect patient privacy. *See infra* Part III.D.1.

43. Thompson & Wohlsen, *supra* note 41.

44. *Id.*

45. Kevin Sack, *Patient Data Posted Online in Major Breach of Privacy*, N.Y. TIMES, Sept. 8, 2011, at A1, http://www.nytimes.com/2011/09/09/us/09breach.html?pagewanted=all.

46. *Id.*

47. *Id.*

sensitive and embarrassing medical conditions, identity theft, medical identity theft,[48] and significant emotional and financial harm to the patient.[49] Privacy concerns can ultimately affect patients' health by deterring them from obtaining medical care or disclosing their medical condition to a healthcare provider. A 2011 study found that patients often consider their privacy when deciding whether to receive care, whether to withhold information from their physician, and where to receive care.[50] Thus, patients' concerns about the privacy of their medical records may have a direct impact on the health care they receive.[51]

---

48. *See* PRIVACY CONSIDERATIONS, *supra* note 2, at 5–6, 9.

49. *See, e.g.*, Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 490 (1995) (describing various harms from patient privacy breaches including insult to dignity, social or psychological harms, stigmatization, and economic harms such as loss of employment, housing, or insurance). Privacy breaches can also lead to identity theft and fraudulent billing for procedures that were never performed. *See* Sack, *supra* note 45, at A1.

50. One survey noted that:

> 27.1 percent of patients stated they would withhold information from their care provider based on privacy concerns. 27.6 percent stated they have or would postpone seeking care for a sensitive medical condition due to privacy concerns. More than 1 out of 2 patients indicated they would seek care outside of their community due to privacy concerns with 35 percent indicating they would travel more than 50 miles. By withholding medical information, patients are impacting the care received and hence the outcome.

PRIVACY CONSIDERATIONS, *supra* note 2, at 4. The survey was presented prospectively, asking respondents how they would potentially change their consumption of healthcare, and thus may overestimate the number of people who would actually withhold information or change where they receive care.

51. EMRs can certainly facilitate breaches of patient privacy. On the other hand, not all patient privacy breaches are facilitated by EMRs, because healthcare providers often store patient records in databases separate from an EMR system. A database separate from an EMR might consist of scanned medical records, a spreadsheet of patient names, or an access database. While an EMR is used for recording real time data, databases are used for storing patient records. Thus, an EMR will have a patient database, while a patient database is not necessarily an EMR. *See* Lisbeth Haines, *EMRs and Database Structures*, BEHAV. HEALTHCARE (Mar. 1, 2007), http://www.behavioral.net/article/emrs-and-database-structures (explaining the different considerations for database structures that can be used to tailor an EMR). For instance, OCR notes the following sources of PHI breaches affecting 500 or more patients since 2009: backup tapes, CDs, computer, servers, emails, EMRs, hard drives, laptops, mailings, x-ray films, portable electronic devices, and paper. *Breaches Affecting 500 or More Individuals*, *supra* note 5. Thus, PHI can be stored in a wide variety of mediums, not limited to EMRs, which can lead to breaches of patient privacy. Furthermore, patient privacy breaches stemming from stolen hardware (e.g. laptops, computers, hard drives, etc.) may be a consequence of the data being stored on that specific type of hardware. The different sources of patient privacy breaches help demonstrate that not all breaches are caused by EMRs, and this may help temper concerns regarding EMRs and patient privacy that are better directed towards patient databases in general.

C. HIPAA Privacy and Security Rules: Current Enforcement

To help protect patient privacy, Congress passed the HIPAA Privacy Rule in 2000, which prohibits the unauthorized disclosures of PHI[52] held by covered entities.[53] The HIPAA Privacy Rule took effect in 2003,[54] and Congress empowered OCR to investigate complaints of patient privacy breaches and impose civil monetary penalties of $100 per failure violation, with penalties of up to $25,000 in a calendar year for identical violations.[55] Individuals who knowingly obtain or disclose PHI can receive up to one-year imprisonment and a $50,000 fine, with increased penalties if the conduct involves false pretenses or intent to sell the PHI.[56] The HITECH Act increased the maximum civil monetary penalty to $50,000 per violation with a $1.5 million yearly cap for identical violations.[57] It also increased the maximum criminal penalty to ten-years imprisonment and a $250,000 fine.[58]

Along with the HIPAA Privacy Rule, Congress passed the HIPAA

---

52. PHI includes all:

> "*Individually identifiable health information*" . . . including demographic data, that relates to:
>
> [1] the individual's past, present or future physical or mental health or condition,
>
> [2] the provision of health care to the individual, or
>
> [3] the past, present, or future payment for the provision of health care to the individual,
>
> and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

OCR PRIVACY BRIEF, *supra* note 7, at 4.

53. HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 (2013); *see* OCR PRIVACY BRIEF, *supra* note 7, at 2–3 (defining covered entities to include health plans, healthcare providers, and healthcare clearinghouses).

54. *See* Standards for Privacy of Individually Identifiable Health Information; Final Privacy Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 164.502–24).

55. OCR PRIVACY BRIEF, *supra* note 7, at 17 ("HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.").

56. One source notes that:

> The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

OCR PRIVACY BRIEF, *supra* note 7, at 18.

57. 42 U.S.C. § 1320d-5(a)(3)(D) (2012).

58. The maximum criminal penalties can apply if the "wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain, or malicious harm." OCR PRIVACY BRIEF, *supra* note 7, at 18.

Security Rule in 2003.[59] The HIPAA Security Rule "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[60] It also addresses topics such as information system reviews (audit logs), assigning unique logins to track system use, password maintenance, protecting computer workstations, and data encryption.[61]

Enforcement of the HIPAA Privacy and Security Rules, however, has generally been lax. OCR typically closes a complaint before conducting an investigation and has levied only one civil monetary penalty.[62] After receiving a HIPAA complaint,[63] OCR performs an intake process and either: (1) closes the complaint; (2) refers the complaint to the Department of Justice; or (3) investigates the allegations in the complaint.[64]

OCR categorizes a case that is closed before an investigation as "resolved," meaning that the complaint was dismissed because it did not properly allege a violation of the Privacy or Security Rule or suffered from a procedural defect.[65] From 2003 to 2013, between 53% and 78% of the total cases OCR categorized as resolved were cases dismissed prior to an investigation.[66] These resolved Privacy and Security Rule complaints suffer a fate similar to complaints dismissed in federal court

59. The HIPAA Security Rule went into effect on April 21, 2005. HIPAA Security Rule, 45 C.F.R. §§ 164.306–18 (2013).

60. *Health Information Privacy: The Security Rule*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html (last visited Sept. 26, 2014).

61. DEP'T OF HEALTH & HUMAN SERVS., HIPAA ADMINISTRATIVE SIMPLIFICATION: REGULATION TEXT 45 CFR PARTS 160, 162, AND 164, at 40–42 (2006), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

62. *See infra* Part I.C.

63. While OCR lumps Privacy and Security Rules complaints into one data set, these complaints result from some type of compromise of patient privacy, even if the alleged violation was a result of the HIPAA Security Rule.

64. *See Health Information Privacy: Enforcement Process*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process (last visited Sept. 26, 2014).

65. After intake and review of a complaint, HHS will dismiss a complaint and consider the dismissal a "Resolution" if: (1) the violation did not occur after April 14, 2003; (2) the entity is not covered by the Privacy Rule; (3) the complaint was not filed within 180 days of the alleged violation and an extension was not granted; or (4) the incident described in the complaint does not violate the Privacy Rule. *Id.*

66. *Health Information Privacy: Enforcement Results by Year*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html (last visited Sept. 26, 2014).

for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6): neither the alleged breach of privacy nor the civil suit may proceed to the investigation or discovery stage to build the factual record.[67] For the cases in which OCR chooses to conduct an investigation, OCR almost always either finds no violation or asks for voluntary compliance.[68] The head of OCR stated that, "our first approach to dealing with any complaint is to work for voluntary compliance."[69]

In eleven years since the Privacy Rule and nine years since the Security Rule took effect,[70] OCR has received nearly 100,000 HIPAA complaints.[71] Moreover, complaints have increased steadily almost every year.[72] In addressing the complaints, OCR has levied one civil

---

67. *See* Arthur R. Miller, *From* Conley *to* Twombly *to* Iqbal*: A Double Play on the Federal Rules of Civil Procedure*, 60 DUKE L.J. 1, 61–71 (2010) (describing the costs of discovery and the *Twombly* Court's "ready acceptance of the blunt instrument of plausibility pleading as a barrier to discovery"); *Enforcement Process*, *supra* note 64 (illustrating how HIPAA complaints resolved after "Intake & Review" do not proceed to an investigation).

68. *See Enforcement Process*, *supra* note 64.

69. Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A01, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672.html; *cf.* Tatiana Melnik & Brian Balow, *When HHS Calls, You Should Answer*, 13 J. HEALTH CARE COMPLIANCE 81, 81 (2011), *available at* http://melniklegal.com/av/2011_JHCC_When_HHS_Calls_Answer.pdf ("Actors in the health care space know that OCR has taken a relatively soft approach to enforcing HIPAA's security requirements . . . .").

70. Covered entities were required to comply with the HIPAA Privacy Rule beginning April 14, 2003 and the HIPAA Security Rule beginning April 21, 2005. *Health Information Privacy: HIPAA Enforcement*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html (last visited Sept. 26, 2014).

71. "[S]ince the compliance date in April 2003, HHS has received over 99,957 HIPAA complaints." *Health Information Privacy: Enforcement Highlights (As of August 31, 2014)*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html (follow "Enforcement Results as of the Date of This Summary" hyperlink) (last visited Sept. 26, 2014).

72. OCR received 6534 HIPAA complaints in 2003 and 12,915 complaints in 2013. The number of complaints has increased each year with the exception of 2008–2009. *Health Information Privacy: Complaints Received by Calendar Year*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html (last visited Sept. 26, 2014). An individual can quickly and easily submit a HIPAA complaint through an online submission form on OCR's website. *Complaint Portal*, DEP'T OF HEALTH & HUMAN SERVS., https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf (last visited Sept. 1, 2014). An individual can also file a complaint by completing and emailing a short "Health Information Privacy Complaint" form to OCR. The complaint form asks for basic information about the patient, the covered entity, and the incident. *Health Information Privacy: How to File a Complaint*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/complaints/ (last visited Sept. 26, 2014). The low barriers to filing a complaint may contribute to the large number of complaints filed each year.

monetary penalty and entered into twenty-one resolution agreements.[73] OCR levied its first and only civil monetary penalty about eight years after the Privacy Rule went in effect, fining Cignet Health in February 2011 for its failure to provide patients access to their medical records.[74] OCR only imposed a civil monetary penalty, however, after Cignet failed to respond to OCR's investigative calls, letters, and eventually a subpoena.[75] Cignet only provided medical records to the forty-one patients who had requested access after a default judgment was entered against it.[76] Even then, Cignet provided the medical records of 4500 patients unrelated to the investigation and for which Cignet had no reason to disclose.[77]

After the entry of default, OCR provided Cignet an opportunity to submit mitigating evidence to reduce or waive any civil monetary penalties.[78] Cignet once again refused to respond to OCR, and six months later, OCR finally levied a total fine for $4.3 million.[79] OCR officials were likely infuriated by the complete lack of response by Cignet, and an OCR spokeswoman said "'this was really willful neglect . . . [t]hey would not respond to the department.'"[80] Of note, Cignet had a checkered past: it had sold health insurance without a license, and its owner lost his physician's license for mail and loan

---

73. *Health Information Privacy: Case Examples and Resolution Agreements*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Sept. 26, 2014) ("A resolution agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement likely would include the payment of a resolution amount. These agreements are reserved to settle investigations with more serious outcomes.").

74. *See* Rebecca C. Fayed, *Heightened HIPAA Enforcement: Ready or Not, Here They Come*, 13 J. HEALTH CARE COMPLIANCE 37, 37–38 (July–Aug. 2011).

75. *Id.* at 38.

76. *Id.*

77. Lena H. Sun, *Clinic Fined $4.3 Million for Failing To Provide Patients' Medical Records*, WASH. POST, Feb. 23, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207094.html.

78. *See* Fayed, *supra* note 74, at 38.

79. OCR was limited by a $1.5 million dollar per calendar year statutory cap. *Id.*

80. Sun, *supra* note 77 (quoting Rachel Seeger, spokeswoman of the Office for Civil Rights). Of the $4.3 million fine, $3 million was for the failure to cooperate with the investigation, and only $1.3 million was for the failure to provide medical records. Notice of Proposed Determination from Georgina C. Verdugo, Dir., Office of Civil Rights, Dep't of Health & Human Servs., to Daniel E. Austin, Cignet Health Ctr., at 2–6 (Oct. 2009), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetpenaltynotice.pdf.

fraud.[81]

OCR asserts that it resolved almost 23,000 cases by requiring covered entities to take corrective actions such as making changes in their privacy practices.[82] Covered entities have taken corrective actions such as repositioning monitors in the waiting room that were once visible to patients and correcting a computer flaw that sent explanations of benefits to the wrong person.[83] A critic of levying fines may contend that requiring corrective action is an effective way of obtaining compliance with HIPAA because it allows covered entities to change their internal policies to better comply with HIPAA regulations moving forward. OCR's reluctance to issue civil monetary penalties, however, does not seem to have provided the proper motivation for healthcare organizations to prevent patient privacy breaches in a digital environment. Compliance under HIPAA has been described as "illusory,"[84] because OCR allows for self-correction rather than levying penalties and fines:

> [A] comparison of the sheer volume of complaints received by the OCR to date significantly overshadows the largely non-existent imposition of any penalties. The significant disparity between the two not only decreases any urgency to comply, but the "[l]ack of enforcement [also] undermines compliance . . . because privacy officers [do not] get budget and management attention unless they can show that the rules have teeth." In short, HIPAA has developed a reputation as a set of standards that is not actively enforced.[85]

In November 2013, the Office of the Inspector General ("OIG") published a report highlighting OCR's shortcomings in overseeing the enforcement of the HIPAA Security Rule.[86] Specifically, the OIG

---

81. Sun, *supra* note 77.

82. *Enforcement Highlights (As of August 31, 2014)*, *supra* note 71.

83. *Health Information Privacy: Case Examples and Resolution Agreements: All Case Examples*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case21 (last visited Sept. 26, 2014).

84. Tobi M. Murphy, *Enforcement of the HIPAA Privacy Rule: Moving from Illusory Voluntary Compliance to Continuous Compliance through Private Accreditation*, 54 LOY. L. REV. 155, 179 (2008).

85. *Id.* at 181 (quoting in part Kim S. Nash & Deborah Gage, *A Tenuous Grip on Data: Medical Data Travels Far and Wide on a Typical Day, Vulnerable at Each Handoff*, BASELINE (Dec. 6, 2006), http://www.baselinemag.com/c/a/Projects-Security/A-Tenuous-Grip-on-Data/ (citation omitted)).

86. Thomas M. Salmon, *The Office of Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule*, DEP'T OF HEALTH & HUMAN SERVS., OFFICE INSPECTOR GEN. (Nov. 2013), *available at* https://oig.hhs.gov/oas/reports/region4/41105025.pdf.

found that OCR was deficient in overseeing the audit process of covered entities[87] and its Security Rule investigations did not contain required documentation.[88] The OIG recommended that OCR takes several steps to better enforce the HIPAA Security Rule.[89]

To OCR's credit, however, it has entered into twenty-one settlement agreements for alleged HIPAA violations as of September 2014.[90] Without admitting liability, covered entities have paid settlements ranging from $35,000 to $4.8 million.[91] OCR entered into nine settlements from June 2013 through June 2014,[92] and a chief regional OCR attorney stated in June 2014 that OCR is likely to increase its HIPAA enforcement over the next twelve months.[93] Although OCR has

---

87. *Id.* at ii ("[OCR] had not assessed the risks, established priorities, or implemented controls for its HITECH requirement to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements. As a result, OCR had limited assurance that covered entities complied with the Security Rule.").

88. The OIG found that OCR's:

> Security Rule investigation files did not contain required documentation supporting key decisions because its staff did not consistently follow OCR investigation procedures by sufficiently reviewing investigation case documentation. OCR had not implemented sufficient controls, including supervisory review and documentation retention, to ensure investigators follow investigation policies and procedures for properly initiating, processing, and closing Security Rule investigations.

Id.

89. The OIG recommended that OCR:

> • assess the risks, establish priorities, and implement controls for its HITECH auditing requirements;
>
> • provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at covered entities;
>
> • implement sufficient controls, including supervisory review and documentation retention,
>
> to ensure policies and procedures for Security Rule investigations are followed; and
>
> • implement the NIST Risk Management Framework for systems used to oversee and enforce the Security Rule

Id. at ii–iii.

90. *See Case Examples and Resolution Agreements*, *supra* note 73.

91. *Health Information Privacy: Data Breach Results in $4.8 Million HIPAA Settlements*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html (last visited Sept. 26, 2014) (describing a $3.3 million settlement with New York and Presbyterian Hospital and another $1.5 million settlement with Columbia University arising from the same potential HIPAA violations); *Health Information Privacy: Resolution Agreement—Management Services Organization Washington, Inc.*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/msoresagr.html (last visited Sept. 26, 2014) (describing $35,000 settlement for potential HIPAA violations).

92. *See Case Examples and Resolution Agreements*, *supra* note 73.

93. *See* Jeff Overley, *Big Year Ahead for HIPAA Fines, HHS Atty Says*, LAW360 (June 12, 2014, 8:19 PM), http://www.law360.com/articles/547721/big-year-ahead-for-hipaa-fines-hhs-

certainly increased the number of settlements it has reached in recent months,[94] the resolution agreements usually result from egregious breaches of patient privacy that oftentimes affect millions of patients.[95] A covered entity that experiences a high profile breach of millions of patient medical records may certainly be the target of an OCR investigation. It remains to be seen, however, whether OCR will actually increase its HIPAA enforcement—for not only high profile breaches affecting millions of patients—in the future. Complaints of patient privacy breaches continue to grow in spite of the potential penalties under the HIPAA Privacy and Security Rules.[96]

II. HITECH AMENDMENTS: EXPANSION OF HIPAA ENFORCEMENT TO STATE ATTORNEYS GENERAL

A. Overview

In addition to providing billions of dollars in incentive payments to promote EMR adoption,[97] the HITECH Act also amended HIPAA in an

---

atty-says.

94. OCR entered into thirteen HIPAA settlement agreements between July 2008 and May 2013, and nine HIPAA settlement agreements between June 2013 and June 2014. *Case Examples and Resolution Agreements*, *supra* note 73.

95. *See, e.g.*, Resolution Agreement, Linda C. Colón, Regional Manager, Office of Civil Rights, Dep't of Health & Human Servs., to Robert E. Kelly, President and Chief Operating Officer, New York and Presbyterian Hospital, at 1, *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf (last visited Sept. 26, 2014) (stating that New York and Presbyterian Hospital (NYP) "impermissibly disclosed the [electronic] PHI of 6,800 patients to Google and other Internet search engines when a computer server that had access to NYP [electronic] PHI information systems was errantly reconfigured"); *Health Information Privacy: HHS Settles HIPAA Case with BCBST for $1.5 Million*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/bcbstagrmnt.html (last visited Sept. 26, 2014) (describing how Blue Cross Blue Shield of Tennessee did not encrypt its hard drives and had fifty-seven computers stolen containing PHI of over 1 million patients); *see also Health Information Privacy: CVS Pays $2.25 Million & Toughens Disposal Practices To Settle HIPAA Privacy Case*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html (last visited Sept. 1, 2014) (discussing CVS Pharmacy alleged disposal of private health information in dumpsters accessible to the public).

96. *See supra* note 72 and accompanying text. *But cf.* Jack Brill, Note, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105, 2123 (2008) ("[G]iven HIPAA's complexity and the discretion that it affords covered entities, it might not be reasonable in all instances for covered entities to be expected to know how to comply with HIPAA's complicated requirements. Indeed, HHS recognized the difficulties in abiding by the Privacy and Security Rules and therefore, rather than first issuing a fine for a violation, it works with a covered entity to achieve compliance.").

97. Yaffee, *supra* note 3, at 356.

attempt to better protect patient privacy in an increasingly digital healthcare environment. The HITECH Amendments strengthened HIPAA's patient privacy protections by: (1) applying HIPAA directly to business associates,[98] (2) requiring covered entities to notify individuals for breaches of unsecured PHI,[99] (3) requiring covered entities to notify prominent media outlets for breaches of 500 or more individuals,[100] and (4) increasing penalties for non-compliance.[101]

The HITECH Amendments also expanded the enforcement powers of HIPAA from OCR to include AGs.[102] AGs can now bring a civil action for violations of HIPAA in federal court and obtain damages on behalf of their residents or enjoin further violations of HIPAA under 42 U.S.C. § 1320d-5(d).[103] Yet, AGs have not embraced their new HIPAA enforcement powers. Only a handful of AGs have filed suit under HIPAA since the HITECH Amendments took effect in 2009. Two suits were brought against the same defendant, Health Net, by the Connecticut AG in 2010 and the Vermont AG in early 2011.[104] Health Net allegedly failed to provide the states with timely notice of a missing

98. Previously, HIPAA only applied directly to healthcare plans, providers and clearinghouses. As a result, contractors, consultants, and third-party administrators (collectively, "business associates") were not subject to oversight by HHS. Instead, the health plan was required to contract for protection of PHI through individual agreements with business associates. *See* Mark Holloway & Edward Fensholt, *HITECH: HIPAA Gets a Facelift*, 22 BENEFITS L.J. 85, 85–86 (2009).

99. *Id.* at 86.

100. *Id.* at 87.

101. *Id.* at 87–88.

102. *See* 42 U.S.C. § 1320d-5(d) (2012).

103. The text of 42 U.S.C. § 1320d-5(d)(1) reads:

> (d) Enforcement by State attorneys general
>
> (1) Civil action
>
> Except as provided in subsection (b), in any case in which the attorney general of a State has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of this part, the attorney general of the State, as parens patriae, may bring a civil action on behalf of such residents of the State in a district court of the United States of appropriate jurisdiction—
>
> (A) to enjoin further such violation by the defendant; or
>
> (B) to obtain damages on behalf of such residents of the State, in an amount equal to the amount determined under paragraph (2).

Id.

104. Kimberly Leonard, *State Attorneys General Not Leaping to Embrace HIPAA Enforcement*, CTR. FOR PUB. INTEGRITY (Sept. 20, 2011, 6:00 A.M.), http://www.iwatchnews.org/2011/09/20/6666/state-attorneys-general-not-leaping-embrace-hipaa-enforcement.

disk drive containing unencrypted PHI.[105] Health Net settled with Connecticut for $250,000 and Vermont for $55,000.[106] Responding to data breaches in 2010 and 2012, the Massachusetts AG filed several HIPAA suits and settled with various defendants for amounts ranging from $140,000 to $750,000.[107] In 2012, the Minnesota AG filed suit under HIPAA against a collection agency, Accretive Health, for allegedly losing a laptop computer containing unencrypted PHI of 23,500 patients.[108] Accretive Health settled with Minnesota for $2.49 million.[109]

B. Attorneys General Will Not Bring Many Suits Under HIPAA

By allowing AGs to file suit for HIPAA violations through the HITECH Amendments, Congress attempted to decrease the burden of HIPAA enforcement on OCR. AGs, however, will not bring many suits under HIPAA and OCR will continue to be inundated with an increasing number of HIPAA complaints. Critics may contend that AGs have not yet been trained on bringing a cause of action under HIPAA and that the number of suits brought by AGs will increase in the near future.[110] But AGs have now had five years to bring suits under

---

105. *Id.*

106. *Id.*

107. *See* Press Release, Mass. Att'y Gen., Former Owners of Medical Billing Practice, Pathology Groups Agree to Pay $140,000 to Settle Claims that Patients' Health Information was Disposed of at Georgetown Dump (Jan. 7, 2013), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-at-dump.html; Press Release, Mass. Att'y Gen., South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations (May 24, 2012), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html; Press Release, Mass. Att'y Gen., Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients (July 23, 2014), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html.

108. Press Release, Office of Minn. Att'y Gen., Attorney General Swanson Sues Accretive Health for Patient Privacy Violation (Jan. 19, 2012), *available at* http://www.ag.state.mn.us/Consumer/PressRelease/120119AccretiveHealth.asp. The Minnesota AG was also the first to file suit against a business associate, as allowed under the HITECH Amendments.

109. Settlement Agreement, Release and Order at 7, Minnesota v. Accretive Health, Inc. (D. Minn. July 30, 2012) (No. 12-145), *available at* http://www.sec.gov/Archives/edgar/data/1472595/000147259512000029/ex991settlementorder.htm.

110. *See* Howard Anderson, *State AGs to Get HIPAA Lawsuit Training*, GOV INFO SEC. (Mar. 10, 2011), http://www.govinfosecurity.com/articles.php?art_id=3418. In the spring of 2011, OCR offered to "pay all expenses for two members of each state's attorney general's office to attend the [HIPAA enforcement] training . . . ." *Id.* The deputy director for health information privacy at OCR stated that after training, the "'state attorneys general will be better prepared to

HIPAA, and only a few AGs have filed HIPAA suits. Even if AGs are untrained in enforcing HIPAA, extra training will not lead to AGs filing more HIPAA suits due to various structural barriers, including: (1) a lack of time and resources among AGs, (2) the low number of patient privacy complaints received by AGs compared to other consumer complaints, (3) the availability of other state law remedies, and (4) the political nature of the AG position. Each barrier is analyzed below.

1. Lack of Time and Resources

AGs face budget cuts and increased workloads, and they also lack the time and resources to investigate HIPAA complaints and to file lawsuits. For example, the Rhode Island AG's Office was understaffed by over fifteen full-time employees in 2004.[111] When adjusted for inflation, the Rhode Island AG's Office received less state funding in 2012 than in 2004.[112] In West Virginia, the caseload of the AG's office increased substantially after the state supreme court adopted a rule requiring the AG's office to respond to every appeal, even if the case is not heard.[113] This new rule increased the Office of the West Virginia AG's workload by six to seven times.[114] California cut AG funding by $70 million over two years, and other cash-strapped states similarly reduced AG funding.[115] In 2012, Illinois AG Lisa Madigan protested

---

carry out their new authority under the HITECH Act in enforcing HIPAA' . . . ." *Id.* (quoting Susan McAndrew). Representatives from forty-five AG offices and the District of Columbia attended the training. Cassandra H. Arriaza & Sarah W. Walsh, *HIPAA Enforcement Trends: Growing Civil Enforcement*, BOS. BAR ASS'N HEALTH L. REP. (Jan. 31, 2013), http://healthlawreporter.bbablogs.org/2013/01/31/hipaa-enforcement-trends-growing-civil-enforcement/.

111. The office staffed 60.2 full-time employees when the office needed 75.75 to handle its workload. AM. PROSECUTORS RES. INST., RHODE ISLAND DEPARTMENT OF THE ATTORNEY GENERAL: WORKLOAD ASSESSMENT 15, *available at* http://www.rijustice.ri.gov/documents/reports/AG%20Caseload%20Final%20Report.pdf (last visited Sept. 26, 2014).

112. *Compare* R.I ATT'Y GEN., STATE OF RHODE ISLAND OFFICE OF ATTORNEY GENERAL 2012 ANNUAL REPORT 24 (2012), *available at* http://www.riag.ri.gov/documents/2012annualreport.pdf (listing $22.2 million in AG state funding in 2012), *with* R.I. BUDGET OFF., BUDGET AS ENACTED 2004, at 25 (2004), *available at* http://www.budget.ri.gov/Documents/Prior%20Year%20Budgets/Operating%20Budget%202004/1_Budget%20as%20Enacted%202004.pdf (listing $18.6 million in AG state funding in 2004). Accounting for inflation, $18.6 million in 2004 is equivalent to about $22.6 million in 2012. *CPI Inflation Calculator*, U.S. DEP'T LAB. BUREAU LAB. STAT., http://www.bls.gov/data/inflation_calculator.htm (last visited Sept. 26, 2014).

113. *See* Ry Rivard, *McGraw Busy After Appeals Revisions*, CHARLESTON DAILY MAIL, Mar. 22, 2011, http://www.charlestondailymail.com/News/statehouse/201103211271?page=2&build=cache.

114. *Id.*

115. Greg Bluestein, *State Budget Cuts Clog Criminal Justice System*, ASSOCIATED PRESS (Oct. 26, 2011), *available at* http://www.nbcnews.com/id/45049812/ns/us_newscrime_and_cou

proposed budget cuts, stating that her office was "starting to deteriorate" because it received less taxpayer money in 2012 than in 1998, and that her staff attorneys had not received raises since 2006.[116] As detailed later in this Article, Massachusetts and its AG are outliers in several respects, and the Massachusetts AG actually received an increase in funding from about $38.4 million in 2012 to $42.8 million in 2014.[117]

Facing limited resources, AGs are likely to be more selective of the cases they investigate and prosecute. Filing a HIPAA complaint in federal court will require AG offices to conduct some type of an investigation to allege specific facts in the complaint and meet the pleading standards of *Ashcroft v. Iqbal* and *Bell Atlantic Corp. v. Twombly*.[118] AGs are not likely to spend their limited time and resources conducting an investigation for specific facts to plead in a federal complaint, especially when those issues can be resolved by a federal agency.[119] The HITECH Amendments simply permit, rather than coerce or even pressure, AGs to file suit for patient privacy violations.

Furthermore, nothing prohibits AGs from directing consumer healthcare privacy complaints to the local branch of the OCR. From the perspective of an AG with limited time and resources, it makes sense to refer allegations of HIPAA violations to a federal agency with more expertise in reviewing patient privacy complaints and handling these

---

rts/t/state-budget-cuts-clog-criminal-justice-system/#.VAoDu1bT0ds.

116. Christopher Wills, *Illinois Attorney General Pushes Back on Budget*, ST. J. REG., Mar. 8, 2012, 12:01 AM, http://www.sj-r.com/top-stories/x570354390/Illinois-attorney-general-pushes-back-on-budget?zc_p=0. The Governor of Illinois noted that the AG's office has additional revenue from lawsuits, but the AGs office contends that the use of funds from lawsuits "comes with many strings attached and can't be used for everyday costs of running the office." *Id.*

117. *Compare* COMMONWEALTH OF MASS., FY 2012 BUDGET (2011), *available at* https://malegislature.gov/Budget/FinalBudget/2012, *with* COMMONWEALTH OF MASS., FY 2014 BUDGET (2013) *available at* https://malegislature.gov/Budget/FinalBudget/2014.

118. Ashcroft v. Iqbal, 556 U.S. 662, 678–81 (2009); Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 556–61 (2007). In *Twombly*, the Supreme Court held that plaintiffs must allege enough facts in their complaint not only to make their claims conceivable, but also to make them "plausible." 550 U.S. at 570. In *Iqbal*, the Supreme Court reiterated that "a pleading that offers 'labels and conclusions' or a 'formulaic recitation of the elements of a cause of action'" will not survive a motion to dismiss. 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555). *Iqbal* and *Twombly* give "district court judges the most powerful case management tool of all-a broader authority to simply dismiss a case outright." Rakesh N. Kilaru, Comment, *The New Rule 12(B)(6):* Twombly, Iqbal, *and the Paradox of Pleading*, 62 STAN. L. REV. 905, 908 (2010).

119. *Cf. infra* text accompanying notes 173–76 (describing the Massachusetts AG's HIPAA suit filed in state court).

types of investigations.[120] Many AGs are not eager to inform their constituents that their offices can now investigate and prosecute HIPAA violations. For example, the Minnesota AG's Office does not inform consumers on its website that HIPAA complaints can be filed with its office.[121] The Illinois AG's website provides a link to the OCR website to file a HIPAA complaint without explaining that consumers can file a complaint directly with the AG.[122] The Vermont AG's website also does not appear to inform consumers that they can file a HIPAA complaint directly with its office.[123]

Although the Massachusetts AG does not appear to specifically direct its consumers to file HIPAA complaints with its office, its website does contain a form to submit healthcare complaints, and consumers can select "Personal Medical Information Issue" as a type of complaint.[124] The Connecticut AG, who filed the first HIPAA complaint, directs consumers to file either with OCR or the AG's office.[125] The

120. OCR has received almost 100,000 HIPAA complaints through August 31, 2014, and conducted thousands of investigations. *See Enforcement Highlights*, *supra* note 71 and accompanying text; *Enforcement Results by Year*, *supra* note 66 and accompanying text.

121. OFFICE OF MINN. ATT'Y GEN., MANAGING YOUR HEALTH CARE 23 (Nov. 2012), *available at* http://www.ag.state.mn.us/brochures/pubmanaginghealthcare.pdf. The Minnesota AG's website does inform consumers about state law restricting the use and dissemination of PHI. *Id.* In June 2014, the Minnesota AG's website was updated to state, "[t]he United States Department of Health and Human Services Office for Civil Rights ('OCR') has primary jurisdiction to oversee and enforce HIPAA." *Id.* at 23. Although the Minnesota AG's Office actually filed suit under HIPAA, its website makes no mention that HIPAA complaints can be filed with its office.

122. *Your Rights Under the Health Insurance Portability and Accountability Act (HIPAA)*, OFFICE OF ILL. ATT'Y GEN., http://www.illinoisattorneygeneral.gov/consumers/HIPAA.pdf (last visited Sept. 26, 2014). Nowhere does the website mention filing a claim directly with the AGs office. To illustrate:

> Further information on how to file a complaint with the OCR may be found at their Web site: www.hhs.gov/ocr/hipaa/. In addition, after the compliance dates above, you have a right to file a complaint directly with the covered entity. You should refer to the covered entity's notice of privacy practices for more information about how to file a complaint with the covered entity. For more information on HIPAA, contact the State Insurance Department or Department of Labor.

Id.

123. OFFICE OF VT. ATT'Y GEN., http://www.atg.state.vt.us (last visited Sept. 26, 2014). The Vermont AG's website appears to make no mention of filing HIPAA complaints with its office. *Id.*

124. *Health Care Services/Insurance Complaint Form*, OFFICE OF MASS. ATT'Y GEN., *available at* https://www.eform.ago.state.ma.us/ago_eforms/forms/hcd_ecomplaint.action (last visited Sept. 26, 2014).

125. *Your Rights Under HIPAA*, OFFICE OF CONN. ATT'Y GEN., http://www.ct.gov/ag/cwp/view.asp?A=2130&Q=296210 (last visited Sept. 26, 2014).

Connecticut AG, however, lists the OCR first, and notes that complaints submitted to the AG must be printed and submitted by mail.[126] Complaints submitted to OCR, on the other hand, may be submitted through an online form or by email.[127] The lack of adequate resources among AG offices, and the optional nature of enforcing HIPAA, suggest that AGs will not bring many suits.

2. Attorneys General Use Federal Consumer Protection Statutes When the Statutes Align with the Types of Complaints They Receive

Notwithstanding their lack of time and resources, AGs are unlikely to file many suits under HIPAA because AGs receive relatively few HIPAA privacy complaints from their constituents.[128] For example, in Illinois, the most common consumer complaints in 2013 were related to: (1) consumer debt (mortgage lending, debt collections credit cards); (2) identity theft (fraudulent credit cards and utility accounts, bank fraud); (3) telecommunications (wireless service, local phone service, cable/satellite); and (4) construction/home improvement (remodeling, roofs/gutters).[129] Between 2006 and 2013, healthcare privacy never appeared on Illinois' list of top ten consumer complaints.[130] In fact, healthcare privacy issues do not appear in the twenty-four topics listed under the "Protecting Consumers" portion of the Illinois AG's website.[131]

Likewise, the New York AG Office's initiatives related to mortgage settlement, debt settlement and collection, and taxpayer protection may

126. *Id.*

127. *How to File a Complaint*, *supra* note 72.

128. As described below, the Massachusetts AG is likely to be an exception.

129. *Madigan: Data Breach, Identity Theft Concerns Spike in Top 10 Complaints for 2013*, OFFICE OF ILL. ATT'Y GEN. (Feb. 11, 2014), http://www.illinoisattorneygeneral.gov/pressroom/2014_02/20140211.html.

130. *Id.*; *see also Protecting Consumers*, OFFICE OF ILL. ATT'Y GEN., http://www.illinoisattorneygeneral.gov/consumers/index.html (last visited Sept. 26, 2014).

131. *Protecting Consumers*, *supra* note 130. The portion of the website does mention "Health Care Assistance," but this refers consumers to information on receiving healthcare benefits to which they are entitled. *Protecting Consumers: Health Care Assistance*, OFFICE OF ILL. ATT'Y GEN., http://www.illinoisattorneygeneral.gov/consumers/healthcare.html (last visited Sept. 26, 2014). As mentioned in Part II.B.1, the Illinois AG website does link to a paragraph regarding the HIPAA Privacy Rule, but this information directs consumers to file a complaint with OCR. *Your Rights Under the Health Insurance Portability and Accountability Act (HIPAA*), *supra* note 122.

suggest which claims its consumers face most often.[132] Additionally, its website[133] links to HIPAA in only one instance, stating that the HIPAA Privacy Rule generally does not treat health insurance discount cards as covered entities.[134] Without a steady stream of patient privacy complaints, it should not come as a surprise that the Illinois and the New York AGs have not filed suit under HIPAA.

Instead, AGs are more likely to exercise their powers under federal consumer protection statutes when the subject matter of the federal statutes addresses common complaints in their jurisdictions. Analyzing the federal statutes AGs used to file consumer protection suits helps illustrate this point. AGs have concurrent power with the federal government to bring causes of action under various consumer protection statutes, including HIPAA.[135] A 2011 study found that AGs have filed suit using nine of sixteen federal consumer protection statutes, bringing a total of 120 lawsuits through 2010.[136] Over three-quarters of the 120 suits filed addressed telemarketing: fifty-one causes of action under the Telemarketing Sales Rule ("TSR") and forty under the Telephone Consumer Protection Act ("TCPA").[137] After telemarketing, the next three most common causes of action included ten suits filed under the

132. *See Initiatives*, OFFICE OF N.Y. ATT'Y GEN., http://www.ag.ny.gov/all-features (last visited Sept. 26, 2014).

133. *See generally Index A to Z*, OFFICE OF N.Y. ATT'Y GEN., http://www.ag.ny.gov/index-a-z (last visited Sept. 26, 2014).

134. OFFICE OF N.Y. ATT'Y GEN., NEW YORK STATE ATTORNEY GENERAL'S ADVERTISING, MARKETING AND PROGRAM GUIDELINES FOR MEDICAL AND PRESCRIPTION DISCOUNT CARDS 10, *available at* http://www.ag.ny.gov/sites/default/files/pdfs/bureaus/health_care/discount_cards_guidelines.pdf (last visited Sept. 26, 2014).

135. *See* Amy Widman & Prentiss Cox, *State Attorneys General's Use of Concurrent Public Enforcement Authority in Federal Consumer Protection Laws*, 33 CARDOZO L. REV. 53, 54 (2011). There are twenty-four statutes that allow state enforcement of federal law, and the Widman & Cox study focused on the following sixteen consumer protection laws, including: RESPA, 12 U.S.C. § 2607(d)(4) (2006); HOEPA, 15 U.S.C. § 1640(e) (2006); CROA, 15 U.S.C. § 1679h (2006); FCRA, 15 U.S.C. § 1681s(c)(1) (2006); CPSIA, 15 U.S.C. § 2073(b) (2006); TSR, 15 U.S.C. § 6103 (2006); Boxing Safety, 15 U.S.C. § 6309 (2006); COPPA, 15 U.S.C. § 6504 (2006); CAN-SPAM, 15 U.S.C. § 7706(f) (2006); FACE, 18 U.S.C. § 248 (2006); Nutrition Labeling Act, 21 U.S.C. § 337(b) (2006); HIPAA, 42 U.S.C. § 1320d-5 (2006); TCPA, 47 U.S.C. § 227(f) (2006); Household Goods Mover Oversight Enforcement and Reform Act of 2005, 49 U.S.C. §§ 14710–14711 (2006); Odometer Act, 49 U.S.C. § 32709(d) (2006); Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of 7, 12, and 15 U.S.C.). Widman & Cox, *supra*, at 65 n.75, 66.

136. At the time of the study, only one cause of action had been brought under HIPAA. As discussed in Part II, *supra*, AGs have filed at least six complaints under HIPAA.

137. Widman & Cox, *supra* note 135, at 72.

Credit Repair Organizations Act ("CROA"), five suits filed under the Free Access to Clinic Entrances ("FACE") Act, and five suits filed under the Home Ownership and Equity Protection Act ("HOEPA").[138] These five statutes account for 92.5% (111 of 120) of all suits brought by AGs under federal consumer protection statutes in the 2011 study, and the three most used statutes account for over 84% (101 of 120) of the suits brought by AGs. AGs filed suit using a federal consumer protection statute 84% of the time under telemarketing ("TSR/TCPA") or credit repair statutes ("CROA").

The AGs in the study filed suit used federal consumer protection statutes when the statutes addressed common complaints in their jurisdictions. As discussed above, consumer debt and telecommunications complaints were the first and third most common types of consumer complaints, respectively, in Illinois in 2013.[139] The Illinois AG's Office brought forty-one individual or multi-state cases using two consumer debt/mortgage statutes (CROA and HOEPA) and two telecommunications statutes (TSR and TCPA).[140] The high volume of consumer debt and telecommunications complaints received in Illinois overlaps with the four federal causes of actions used by the Illinois AG.

The suits filed by the Colorado AG also appear to align with common consumer complaints in Colorado. Between 2003 and 2010, the Colorado AG used a single federal consumer protection statute, CROA, to file three individual lawsuits.[141] Consumer debt complaints are prevalent enough in Colorado to appear as one of nine topics listed under a section titled "File Consumer Complaint" on the AG's website.[142] The Missouri AG brought seven individual or multi-state cases under federal telemarketing statutes,[143] and telemarketing complaints are prevalent enough in Missouri that the AG dedicated an entire page titled "No Call Home Page" describing the "No Call List"

138. *Id.*

139. *Madigan: Data Breach, Identity Theft Concerns Spike in Top 10 Complaints for 2013*, *supra* note 129.

140. Widman & Cox, *supra* note 135, at 76.

141. *Id.*

142. *File Consumer Complaint*, OFFICE OF COLO. ATT'Y GEN., https://www.coloradoattorneygeneral.gov/complaint (last visited Sept. 26, 2014). The Colorado AG does not list top complaints for a given year on his website. *Id.*

143. Widman & Cox, *supra* note 135, at 76.

and explaining how to file a complaint against telemarketers.[144]

In sum, AGs may be more likely to use a federal consumer protection statute when the statute aligns with common consumer complaints within their state. It makes sense that AGs exercise their authority under federal law when the laws help address their constituents' most common complaints. Patient privacy breaches may fall under the purview of the consumer protection power of AGs, but patients usually file complaints with OCR[145] rather than their state AG, thereby reducing the number of complaints that AGs receive. While the Massachusetts AG has filed multiple suits under HIPAA,[146] its office established a Health Care Division that "receives and responds to thousands of helpline calls and written complaints each year."[147]

Because AGs do not receive a high volume of patient privacy complaints relative to other types of complaints,[148] it is unlikely that AGs will enforce the HIPAA Privacy and Security Rules.[149]

3. Availability of Other State Law Remedies

It is also unlikely that AGs will file suit under HIPAA because they have common law causes of action and state statutes available to

---

144. *Missouri No Call*, OFFICE OF MO. ATT'Y GEN., http://ago.mo.gov/nocalllaw/nocalllaw.htm (last visited Sept. 26, 2014). The Missouri AG lists the top ten complaints for 2010–2012, with "No-Call Complaints" topping the list in 2011 and 2012. *See Top 10 Complaints: 2012 Top 10 Complaints*, OFFICE OF MO. ATT'Y GEN., http://ago.mo.gov/consumercomplaints/topten/index.htm (last visited Sept. 26, 2014).

145. *See supra* Part II.B.1.

146. *See supra* note 107 and accompanying text.

147. *The Health Care Division*, OFFICE OF MASS. ATT'Y GEN., http://www.mass.gov/ago/bureaus/public-protection-and-advocacy/the-health-care-division/ (last visited Sept. 26, 2014). Because the Massachusetts AG solicits and receives thousands of healthcare calls and complaints each year, it does not come as a surprise that its office has filed multiple suits under HIPAA.

148. For example, patient privacy complaints did not appear in the top ten consumer complaints for states including Illinois, North Carolina, Missouri, Arizona, New York, and Indiana. *See AG Releases Top 10 List of Complaints, Tips*, OFFICE OF IND. ATT'Y GEN. (Mar. 8, 2012), http://www.in.gov/activecalendar/EventList.aspx?view=EventDetails&eventidn=54287&information_id=108902&type=&syndicate=syndicate; *Protecting Consumers*, *supra* note 130; *Top 10 Complaints*, *supra* note 144; *Top Ten Consumer Complaints of 2011*, OFFICE OF N.C. ATT'Y, http://www.ncdoj.gov/getdoc/152dcd47-ee39-475f-b4de-c35a2d8b0c45/Top-Ten-Consumer-Complaints-of-2011-%281%29.aspx (last visited Sept. 26, 2014); *Top 10 Consumer Scams*, OFFICE OF ARIZ. ATT'Y GEN., http://www.azag.gov/consumer/TopTenScams.pdf (last visited Sept. 26, 2014).

149. If consumers are aware that AGs can enforce HIPAA, it is likely that they will file more complaints with AGs, and in turn, AGs may enforce HIPAA more regularly. In Part III.C.1, *infra*, I discuss how partnering state health agencies with AGs may lead to more consumers filing HIPAA complaints with AGs and better institutional enforcement of HIPAA.

address patient privacy breaches.[150] Furthermore, the HIPAA Privacy Rule does not preempt state laws providing greater patient privacy protection; instead, it simply creates a floor for privacy rights.[151] Even if an AG were to file suit under HIPAA, the AG would have likely filed suit absent his or her expanded HIPAA enforcement powers, and the HITECH Amendments are unlikely to cause AGs to file any unique suits under HIPAA. On the other hand, HIPAA may benefit AGs by providing them with the potential to extract additional settlement dollars from defendants and by giving them the ability to file suit in federal court.[152]

Even after the HITECH Amendments permitted them to file suit using HIPAA, AGs have filed suit for breaches of patient privacy relying solely on state law. For example, the Indiana AG sued health insurer WellPoint in October 2010 in state court when the PHI of over 32,000 Indiana patients was made publicly available through the manipulation of a website URL.[153] After it received notification of the breach, WellPoint allegedly did not notify patients for nearly four months.[154] Under the HIPAA Privacy Rule, the Indiana AG could have sued for a violation of HIPAA's Breach Notification Rule, which requires covered entities to provide notice to those affected by a breach within sixty days following discovery of the breach.[155] Instead, the Indiana AG relied exclusively on the Indiana Disclosure of Security

150. *See generally* Beverly Cohen, *Reconciling the HIPAA Privacy Rule with State Laws Regulating* Ex Parte *Interviews of Plaintiffs' Treating Physicians: A Guide to Performing HIPAA Preemption Analysis*, 43 HOUS. L. REV. 1091 (2006).

151. *See Does the HIPAA Privacy Rule Preempt State Laws?*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/faq/preemption_of_state_law/399.html (last visited Sept. 26, 2014) ("The HIPAA Privacy Rule provides a Federal floor of privacy protections for individuals' individually identifiable health information . . . ."). In general, the Privacy Rule will preempt any contrary state law. *See id.* However, "[s]tate laws that relate to the privacy of individually identifiable health information and are both contrary to and more stringent than the Privacy Rule will continue to stand." *How Do Other Privacy Protections Interact With the Privacy Rule?*, NAT'L INST. OF HEALTH, http://privacyruleandresearch.nih.gov/pr_05.asp (last visited Sept. 26, 2014).

152. It remains speculative whether AGs will actually use HIPAA to gain leverage in settlement negotiations or to gain access to a federal court. *See infra* pp. 204–05.

153. Complaint ¶¶ 5–8, Indiana v. Wellpoint, Inc., No. 49D06-1010-PL-47381 (Ind. Cir. Ct. Oct. 29, 2010) [hereinafter Indiana Complaint], *available at* http://www.huntonfiles.com/files/webupload/PrivacyLaw_WellPoint_Complaint.pdf.

154. *Id.* ¶¶ 9–13.

155. *Breach Notification Rule*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html (last visited Sept. 26, 2014).

Breach Act[156] to address Wellpoint's failure to notify it and the affected customers of the breach in a timely manner.[157] WellPoint eventually settled with the Indiana AG for $100,000 and agreed to reimburse costs to the victims of identity theft.[158] Filing suit under state law rather than HIPAA provided the Indiana AG several benefits: familiarity with the state statute, the Indiana state court system,[159] as well as increased state law penalties.[160]

Other states also have statutes under which AGs can file complaints in state court for patient privacy breaches.[161] Four AGs that filed complaints under HIPAA also used parallel state law causes of action. On January 13, 2010, Connecticut AG Richard Blumenthal became the first AG to file a complaint under HIPAA in *Connecticut v. Health Net*.[162] Health Net allegedly lost a computer disk drive containing the PHI, including social security numbers and bank account numbers, of 446,000 enrollees and failed to notify the required parties in a timely fashion.[163] Blumenthal filed a complaint in U.S. District Court under the HIPAA Security Rule,[164] alleging that Health Net failed to protect the confidentiality of electronic PHI against reasonably anticipated threats.[165] The complaint also alleged violations of state law for unfair trade practices.[166] The state law claims allowed Blumenthal to file suit

156. IND. CODE § 24-4.9-2-1 to 11 (West. Supp. 2013).

157. Indiana Complaint, *supra* note 153, ¶¶ 22–23.

158. *Attorney General Reaches Settlement with WellPoint in Consumer Data Breach*, OFFICE OF IND. ATT'Y GEN. (July 5, 2011), http://www.in.gov/portal/news_events/71252.htm.

159. *See, e.g.*, Scott M. Matheson, Jr., *Constitutional Status and Role of the State Attorney General*, 6 U. FLA. J.L. & PUB. POL'Y 1, 3 (1993) (describing the role of the state attorney general including "representing the state, state agencies, and state officers in litigation; enforcing state civil and criminal law"). Given the role of an AG as an enforcer of state law, AGs are likely more familiar with state law and state court than federal law and federal court. *See generally id.* at 3–4.

160. The Indiana AG was able to pray for relief of $300,000: $150,000 for the failure to notify Indiana residents without unreasonable delay and another $150,000 for the failure to notify the Indiana AG without unreasonable delay. Indiana Complaint, *supra* note 153, at 5–6.

161. *See infra* Part.II.B.3 (describing state statutes in Connecticut, Vermont, and Minnesota used by AGs to bring causes of action for patient privacy breaches).

162. Complaint, Connecticut v. Health Net of the Ne., Inc., No. 3:10-cv-00057-PCD (D. Conn. Jan. 13, 2010) [hereinafter Connecticut Complaint], *available at* https://www.huntonprivacyblog.com/uploads/file/CT%20AG%20Complaint%20Against%20Health%20Net.pdf.

163. *Id.* ¶¶ 12–21.

164. *Id.* ¶¶ 25–26 (citing 45 C.F.R. pt. 164 (2010)).

165. *Id.* ¶ 26(f).

166. *Id.* ¶¶ 27–34 (alleging a violation of Connecticut General Statute section 42-110b for unfair trade practices and a violation of Connecticut General Statute section 42A-110b for a willful violation of the unfair trade practices statute).

for the breach of personal information and Health Net's delay in disclosing the breach of security.[167] Even without the power to file suit under HIPAA, Blumenthal could have filed suit using exclusively state law causes of action.[168]

Health Net's loss of the disk drive containing PHI also affected patients in Vermont. Vermont AG William Sorrell followed Blumenthal's lead and filed suit in federal court against Health Net under the HIPAA Security Rule.[169] Sorrell also filed causes of action for the violation of two state statutes—the Vermont Security Breach Notice Act[170] and the Vermont Consumer Fraud Act[171]—for Health Net's alleged misrepresentation of the risks its customers faced due to the compromised PHI and its failure to maintain minimum-security standards that led to the breach.[172] Like Blumenthal, Sorrell could have filed suit for Health Net's alleged patient privacy breach using exclusively state law.

In Massachusetts state court, AG Martha Coakley filed several suits using HIPAA and also alleged state law causes of action. Coakley sued two separate hospitals for the loss of unencrypted back-up tapes containing PHI[173] as well a group of pathology companies in 2012 for their role in the disposal of 67,000 medical records in a public dumpster.[174] In each of the three cases, Coakley alleged a violation of Massachusetts state law in addition to a violation of HIPAA. For example, in her suit against a group of pathology companies, Coakley alleged that the defendants violated HIPAA by, *inter alia*, failing to

---

167. *Id.* ¶¶ 30–31. The Connecticut AG also could have alleged a federal cause of action for failing to comply with the HIPAA Breach Notification Requirements. *See Breach Notification Rule*, *supra* note 155 (follow "Breach Notification Requirements" hyperlink) (discussing notification requirements).

168. HIPAA did provide for greater monetary damages of $10,000 per violation compared to $5000 per violation under the Connecticut statute. *See infra* notes 184–85 and accompanying text.

169. Complaint ¶¶ 25–28, Vermont v. Health Net, Inc., No. 2:11-cv-00016-wks (D. Vt. Jan. 14, 2011) [hereinafter Vermont Complaint], *available at* http://www.atg.state.vt.us/assets/files/Health%20Net%20Compliant%20Filed.pdf.

170. *Id.* ¶¶ 29–31 (citing VT. STAT. ANN. tit. 9, § 2435 (2010)).

171. *Id.* ¶¶ 32–34 (citing VT. STAT. ANN. tit. 9, § 2453 (2010)).

172. Vermont Complaint, *supra* note 169, ¶ 34.

173. *See* Press Release, Mass. Att'y Gen., South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations, *supra* note 107; Press Release, Mass. Att'y Gen., Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations, *supra* note 107.

174. Complaint ¶¶ 1–8, Massachusetts v. Gagnon, No. 12-4568 (Mass. Super. Ct. Dec. 20, 2012), *available at* http://privacylaw.proskauer.com/files/2013/01/Goldthwait.pdf.

implement appropriate safeguards and policies which allowed the PHI to be placed in a public dumpster.[175] Against the same defendants, Coakley also alleged a violation of the Massachusetts Security Breach Act for their failure to implement a comprehensive information security program.[176]

Recently, Minnesota AG Lori Swanson became the first AG outside of the Northeast to file a HIPAA suit, suing Accretive Health in federal court on January 19, 2012.[177] Swanson alleged that Accretive Health contracted to collect debts for Fairview Hospital, acquired PHI and other financial records of thousands of Fairview patients, and that a laptop computer containing unencrypted PHI was stolen from an Accretive Health employee's rental car.[178] Swanson filed suit under the HIPAA Security Rule alleging that Accretive Health failed to comply with HIPAA's security standards, which led to the patient privacy breach.[179] Like the Connecticut, Vermont, and Massachusetts AGs, Swanson also filed state law causes of action, using the Minnesota Health Records Act[180] to allege that Accretive Health unlawfully released health records, the Minnesota Debt Collection Laws,[181] and the Minnesota Prevention of Consumer Fraud Act and Uniform Deceptive Trade Practices Act[182] to allege that Accretive Health mislead patients about its role in the patients' health care.

In each of the cases described above, the AG could have filed suit using related state law claims instead of HIPAA. The availability of state law causes of action for patient privacy breaches suggests that AGs will not file suit under HIPAA that they could not have brought prior to the HITECH Amendments. Thus, HIPAA may not incentivize AGs to bring additional suits because the AGs could have already brought those suits under state law.

The availability of HIPAA, however, may assist AGs by allowing them to extract larger settlements and providing federal court as a

175. *Id.* ¶¶ 93–97.

176. *Id.* ¶¶ 86–92 (citing MASS. GEN. LAWS ch. 93H (2012)).

177. Complaint, Minnesota v. Accretive Health, Inc., No. 0:12-cv-00145-RHK-JJK (D. Minn. Jan. 19, 2012) [hereinafter Minnesota Complaint], *available at* https://www.ag.state.mn.us/PDF/Consumer/AccretiveHealth20120119.pdf.

178. *Id.* ¶¶ 38–43.

179. *Id.* ¶¶ 63–66.

180. *Id.* ¶¶ 67–71 (citing MINN. STAT. § 144.291 (2010)).

181. *Id.* ¶¶ 72–86 (citing MINN. STAT. § 332.31 (2010)).

182. *Id.* ¶¶ 87–98 (citing MINN. STAT. § 325F.69 (2010)).

potential venue. AGs can add HIPAA as an additional cause of action for many patient privacy breaches, and this may result in higher settlements for cases in which HIPAA provides greater monetary damages than state statutes. For example, Connecticut's AG settled with Health Net for $250,000 after alleging Health net violated HIPAA and state law.[183] While Connecticut law provided damages of $5000 per willful violation,[184] HIPAA provided damages of $10,000 per willful violation.[185] HIPAA, however, sets a statutory cap on damages and does not provide for attorney's fees, while some state law causes of action have higher caps on damages[186] and provide for attorney's fees.[187] Although there is insufficient evidence that AGs obtain higher settlements using HIPAA due to the small sample size of cases, it is plausible that HIPAA can help AGs extract more settlement dollars from defendants.

AGs can also file in federal court by alleging a HIPAA violation. As mentioned above, AGs may prefer to file in state court due to their familiarity with state court rules of procedure and state statutes. In some cases, however, federal court may provide advantages over state court. For example, an AG may want to file suit in federal court to broaden the jury pool[188] when suing a community hospital with a

183. Press Release, Office of Conn. Att'y Gen., Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info (July 6, 2010), *available at* http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

184. Connecticut law bars "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." CONN. GEN. STAT. § 42-110b(a) (2012). The state AG can seek damages as great as $5000 for each willful violation. *Id.* § 42-110o(b).

185. 42 U.S.C. § 1320d-5(a)(3)(C) (2012).

186. *See* LA. REV. STAT. ANN. § 22:1023(F)(2)(b)(i) (West. Supp. 2014) (providing for the greater of $100,000 or actual damages suffered for the willful collection or disclosure of genetic information); *see also* JOY PRITTS ET AL., 1 THE STATE OF HEALTH PRIVACY: A SURVEY OF STATE HEALTH PRIVACY STATUTES 159 (2d ed. 2002), *available at* http://sharps.org/wp-content/uploads/PRITTS-REPORT1.pdf (citing the Louisiana law).

187. *See* Pachowitz v. LeDoux, 666 N.W.2d 88, 91 (Wis. Ct. App. 2003) (affirming attorney's fee award of $30,460 under Wisconsin Statute section 895.50 for EMT's disclosure to a third party the reason plaintiff required medical attention).

188. *See* HOWARD M. ERICHSON, INSIDE CIVIL PROCEDURE: WHAT MATTERS AND WHY 210 (2d. ed. 2012). Professor Erichson explains

> [M]any trial lawyers would agree that a jury pool as a whole may have demographic characteristics that make it more favorable for a particular litigant. Federal district courts draw jury pools from a broader area; differences in jury pools tend to be most pronounced in state courts in which jurors are selected from the specific county in which the court is located. Some courts develop reputations among lawyers as being relatively plaintiff-friendly or defendant-friendly based in part on jury demographics.

Id.

positive reputation.[189] Despite HIPAA providing an alternative forum to state court and potentially providing greater damages, it is unlikely that AGs will bring additional suits under HIPAA that they would have not already filed due to the availability of other state law remedies for patient privacy violations.

4. Attorneys General Are Political in Nature

Finally, AGs are not likely to file suit under HIPAA because many HIPAA suits will not benefit their political aspirations. AGs are elected in forty-three out of fifty states and often use their positions as a springboard to run for higher elected office and are thus selective about the cases they choose to pursue.[190] While certain violations of patient privacy may be so egregious that it may be politically beneficial for an AG to bring suit, as described above, AGs will already have a cause of action under state law and will not need to rely on HIPAA.[191] Furthermore, AGs may overlook many patient privacy violations due to the availability of higher profile suits that will build an AG's resume for a reelection bid or a campaign for higher office.[192] As mentioned above, local hospitals may have a positive reputation within a community, which may serve as another disincentive for an AG to sue a hospital.

The political nature of the AG position attracts individuals who run

189. Hospitals can have a positive reputation within a community, and hospitals spend resources in an effort to build and protect their reputation throughout the community. *See, e.g.*, Judith H. Hibbard, Jean Stockard & Martin Tusler, *Hospital Performance Reports: Impact on Quality, Market Share, and Reputation*, 24 HEALTH AFF. 1150 (2005).

190. *See* Colin L. Provost, *State Attorneys General, Entrepreneurship, and Consumer Protection in the New Federalism*, 33 PUBLIUS 37, 39–40 (2003) (describing the political nature of the AG position and noting that "because the office often serves as a springboard into higher political positions, AGs have strong incentives to build up their record of political accomplishment by helping consumers and pursuing high levels of enforcement.").

191. *See supra* Part II.B.3.

192. New York AG Eliot Spitzer provides an example. Spitzer targeted Wall Street fraud and was described as aggressively using his position "to raise his political profile at the expense of high profile companies." Kulbir Walha & Edward E. Filusch, *Eliot Spitzer: A Crusader Against Corporate Malfeasance or a Politically Ambitious Spotlight Hound? A Case Study of Eliot Spitzer and Marsh & McLennan*, 18 GEO. J. LEGAL ETHICS 1111, 1111 (2005) (footnote omitted). Spitzer was elected Governor of New York in 2007 and resigned in 2008 after being exposed for his participation in a prostitution ring. *See* David Kocieniewski & Danny Hakim, *Felled by Scandal, Spitzer Says Focus is on His Family*, N.Y. TIMES, Mar. 13, 2008, at A1, http://www.nytimes.com/2008/03/13/nyregion/13spitzer.html?pagewanted=all&_r=0 (describing how Spitzer's "rise to political power as a fierce enforcer of ethics in public life" helped him get elected "into the governor's office in a landslide").

for higher office.[193] For example, a 2005 study found that more than 40% of AGs since 1980 have run for higher office.[194] Recently, Virginia AG Ken Cuccinelli ran for Governor of Virginia in 2013.[195] New York AG Eliot Spitzer used a "strategic application of state law in an attempt to force systemic changes in financial governance" and was later elected governor of New York.[196] Connecticut AG Richard Blumenthal successfully ran for the U.S. Senate in 2010.[197]

Although Blumenthal actually filed a HIPAA complaint to support his bid for Congress, a unique set of circumstances led him to file suit. Blumenthal announced his intention to run for the U.S. Senate on January 6, 2010,[198] one week before he became the first AG to file a suit under HIPAA.[199] After he filed suit, the Connecticut AG's Office immediately issued a press release noting that this was "the first action by a state attorney general involving violations of HIPAA since the Health Information Technology for Economic and Clinical Health Act (HITECH) authorized state attorneys general to enforce HIPAA."[200] As the first AG to file suit under HIPAA, Blumenthal reinforced his self-described commitment to "aggressive law enforcement for consumer protection, environmental stewardship, labor rights and *personal privacy*, [which] has helped reshape the role of state attorneys general

193. Provost, *supra* note 190, at 38.

194. Justin O'Brien, *The Politics of Enforcement: Eliot Spitzer, State-Federal Relations, and the Redesign of Financial Regulation*, 35 PUBLIUS 449, 465 (2005).

195. Anita Kumar, *Ken Cuccinelli Announces He Will Run for Va. Governor in 2013*, WASH. POST, Dec. 1, 2011, 4:11 PM, http://www.washingtonpost.com/blogs/virginia-politics/post/ken-cuccinelli-announces-he-will-run-for-va-governor-in-2013/2011/12/01/gIQAH2kjHO_blog.html. Cuccinelli lost in a close race to Terry McAuliffe. *See* Marc Fisher, *McAuliffe Narrowly Wins Va. Governor's Race*, WASH. POST, Nov. 6, 2013, http://www.washingtonpost.com/local/virginia-politics/polls-open-across-virginia-in-hotly-contested-governors-race/2013/11/04/06c6205c-45d2-11e3-bf0c-cebf37c6f484_story.html.

196. O'Brien, *supra* note 194, at 449.

197. David M. Halbfinger, *Blumenthal Wins in Connecticut to Take Dodd's Senate Seat*, N.Y. TIMES, Nov. 2, 2010, at P12, http://www.nytimes.com/2010/11/03/nyregion/03ctsen.html?_r=0.

198. John Christoffersen & Susan Haigh, *Chris Dodd Retiring From Senate; Richard Blumenthal, Attorney General, Will Run*, HUFF. POST (Jan. 6, 2010), http://www.huffingtonpost.com/2010/01/06/chris-dodd-retiring-from-_n_413291.html.

199. Blumenthal filed suit against Health Net on January 13, 2010. *See* Connecticut Complaint, *supra* note 162.

200. Press Release, Office of Conn. Att'y Gen., Attorney General Sues Health Net For Massive Security Breach Involving Private Medical Records And Financial Information On 446,000 Enrollees (Jan. 13, 2010), *available at* http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=453918.

nationwide."[201] Blumenthal may have strategized to file the first suit under HIPAA with his brother, Dr. David Blumenthal, who was the National Coordinator for Health IT at the time.[202] The timing of Blumenthal's HIPAA suit shortly after his Senate campaign announcement, the opportunity to bolster his self-described image as an enforcer of "personal privacy," and his family connection to a prominent healthcare insider familiar with HIPAA all provided him with the opportunity to become the first AG to file a suit under HIPAA and further support his bid for higher office. Other AGs will no longer have a "trailblazer" title in filing a HIPAA suit and will instead focus on the high profile consumer complaints in their states, like mortgage fraud, consumer lending protection, and telemarketing.

Like Blumenthal, Massachusetts AG Martha Coakley, who announced her bid for Governor in 2013,[203] also faced a unique set of circumstances that encouraged her to file multiple HIPAA suits in state court. Massachusetts is committed to health care, passing legislation providing universal health insurance coverage for its residents in 2006[204] and establishing a specific Health Care Division of the AG's office in 2007.[205] Along with increased funding for her office,[206] Coakley's office solicits and receives thousands of healthcare complaints[207] that may align HIPAA with the type of complaints her office receives, and ultimately make it politically beneficial to file suit for violations of patient privacy under HIPAA and state law. When running for reelection or higher political office, other AGs are not likely to file suit for privacy complaints under HIPAA due to the low volume of complaints they receive, their limited time and resources, and the fact that they usually file suit in the types of cases that their residents

201. *Richard Blumenthal*, OFF. OF CONN. ATT'Y GEN., http://www.ct.gov/ag/cwp/view.asp?A=2178&Q=295440 (emphasis added) (last updated Jan. 23, 2008, 2:09:23 PM).

202. Marianne Kolbasuk McGee, *National Health IT Coordinator Blumenthal Stepping Down*, INFORMATIONWEEK GOV'T (Feb. 3, 2011, 8:24 PM), http://www.informationweek.com/government/leadership/national-health-it-coordinator-blumenthal-stepping-down/d/d-id/1095881.

203. *See* Frank Phillips, *Coakley in Governor's Race, with Backing, Baggage*, BOS. GLOBE, (Sept. 15, 2013), http://www.bostonglobe.com/metro/2013/09/15/coakley-join-race-for-governor-monday/WSjVtXrvn7mw9ck5MF8k6I/story.html.

204. KAISER FAMILY FOUND., MASSACHUSETTS HEALTH CARE REFORM: SIX YEARS LATER 1 (May 2012), *available at* http://kaiserfamilyfoundation.files.wordpress.com/2013/01/8311.pdf.

205. *See supra* note 147 and accompanying text.

206. *See supra* note 117 and accompanying text.

207. *See supra* note 147 and accompanying text.

encounter most often.[208]

A survey of press releases from different AGs may illustrate the types of cases that AGs believe their constituents care most about, and in turn may provide talking points for AGs in their campaigns. In 2012, AGs issued press releases with headlines related to: identity theft, illegal synthetic drugs, settlements with banks, and returning wage and benefits to workers in Illinois[209] and mortgage investigations, the prescription drug crisis, identity theft, and rental scams in New York.[210] Neither of those states issued press releases related to patient privacy protection.[211] While the absence of press releases regarding healthcare privacy could be the result of several different factors,[212] as explained in Part II.B.2, AGs do not receive many patient privacy complaints relative to other complaints, and the press releases may reflect the issues AGs feel are most salient to their constituents.[213]

AGs may also be deterred from suing hospitals with positive reputations.[214] An AG with aspirations for higher political office would likely have to proceed with caution when deciding whether to file suit against a reputable hospital under HIPAA. While AGs may file certain types of suits in order to appear as consumer advocates, patient privacy usually falls near the bottom of the list, and AGs will not rush to enforce HIPAA.

---

208. *See supra* Parts II.B.1–2.

209. *E.g.*, *Press Room—February 2012*, OFFICE OF ILL. ATT'Y GEN., http://www.illinoisattorneygeneral.gov/pressroom/2012_02/index.html (last visited Sept. 26, 2014).

210. *E.g.*, *Press Releases*, OFFICE OF N.Y. ATT'Y GEN., http://www.ag.ny.gov/press-releases-for-year/2012?page=2 (last visited Sept. 26, 2014).

211. The Minnesota AG, however, issued a press release regarding the HIPAA suit against Accretive Health. Press Release, Office of Minn. Att'y Gen., *supra* note 108.

212. It is possible that AGs receive consumer complaints regarding patient privacy, take action on these complaints, and yet choose not to issue a press release. The relatively few number of patient privacy complaints received by AGs, however, makes it likely that AGs have either not taken action against many patient privacy complaints or do not perceive patient privacy as salient enough to their constituents to issue a press release.

213. *See, e.g.*, Sooyoung Cho & William Benoit, *2004 Presidential Campaign Messages: A Functional Analysis of Press Releases from President Bush and Senator Kerry*, 32 PUB. REL. REV. 47 (2006) (explaining how press releases can be used to highlight a candidate's past accomplishments and future goals); *see also* M. Mark Miller et al., *Framing the Candidates in Presidential Primaries: Issues and Images in Press Releases and News Coverage*, 75 JOURNALISM MASS COMM. Q. 312 (1998).

214. Hospitals often work hard to build and maintain a positive reputation within their community to maintain customer loyalty and market share. "If a hospital's reputation is affected, it may eventually experience market share declines via consumer choice, purchaser choice, or physician referral." *See* Hibbard, Stockard & Tusler, *supra* note 189, at 1151.

III. IMPROVING HIPAA ENFORCEMENT AND PROTECTING PATIENT PRIVACY

A. Overview

The number of patient privacy complaints continues to increase: OCR received nearly 10,000 HIPAA complaints during the first eight months of 2014.[215] While both OCR and AGs have the power to punish HIPAA violations, HIPAA lacks strong institutional enforcement.[216] Although HIPAA provides patient privacy protection on paper, actually delivering substantive protection will require both increased institutional enforcement of HIPAA and other complementary initiatives and security requirements.

First, in identifying potential solutions to better protect patient privacy, I propose a new framework for evaluating different types of privacy breaches and solutions. This analytical framework distinguishes between different types of patient privacy breaches based upon the willful, negligent, or non-negligent conduct of an individual or healthcare organization. These distinctions demonstrate that different enforcement mechanisms may be better suited for addressing specific types of breaches.

Next, given the structural barriers that OCR and AGs face in enforcing HIPAA, I propose a solution for strengthening the institutional enforcement of HIPAA through partnerships between state health agencies and AGs to solicit and investigate patient privacy complaints combined with considering limited private rights of action. Finally, I explore complementary approaches to enhanced institutional enforcement of HIPAA, including requiring data encryption of patient records, conducting more audits of covered entities without notice, and some of the mechanisms within the HITECH Amendments that will help better protect patient privacy from different types of breaches.

---

215. OCR received 99,957 total complaints as of August 31, 2014, and 90,001 total complaints as of December 31, 2013. *Enforcement Highlights (As of August 31, 2014)*, *supra* note 71; *Enforcement Highlights (As of December 31, 2013)*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/12312013.html (last updated Jan. 8, 2013) (follow "Enforcement Results as of the Date of This Summary" hyperlink).

216. OCR has levied one civil monetary penalty and reached settlement twenty-one times after receiving nearly 100,000 HIPAA complaints of patient privacy violations. *See supra* notes 71, 73 and accompanying text. Only a few AGs have brought causes of action under HIPAA since being given the enforcement power in 2009. For the reasons articulated in Part II, it is unlikely that AGs will bring many more HIPAA suits.

B. Establishing a Framework for Distinguishing Different Types of Patient Privacy Breaches

Patient privacy breaches can result from a variety of different activities. I classify these activities into three categories, depending on the culpability of the healthcare institution or employee that leads to the breach: (1) Willful, (2) Negligent, and (3) Non-Negligent. In other words, these categories focus on the liability from the perspective of the covered entity, business associate, or employee. First, a willful breach occurs when an employee of a covered entity or business associate purposefully violates HIPAA through unauthorized access or disclosure of PHI.[217] Next, a negligent breach occurs when the careless action of a healthcare institution or employee compromises patient privacy.[218] A negligent breach can also reflect a healthcare institution's inadequate security procedures. Finally, a non-negligent breach occurs when a covered entity or business associate is the victim of a breach that reasonable security measures may not have prevented.[219] The distinction between these types of breaches is important because some solutions may only address one or two types of breaches.

Type of Breach	Description	Example	Solution
1) Willful	Employee intentionally violates HIPAA through unauthorized access or disclosure of patient information	Employee looks at Britney Spears's or ex-wife's EMR out of curiosity or for personal gain	State Health Agency–AG partnership; Limited Private Right of Action; Audits without Notice
2) Negligent	Negligent action of hospital/employee or inadequate security procedure leads to the compromise of patient data	Company accidentally posts patient information online; hospital accidentally makes patient information viewable in the waiting room	State Health Agency–AG partnership; Limited Private Right of Action; Audits without Notice
3) Non-Negligent	Covered entity is the victim of a breach that reasonable security measures may not have prevented	Thief breaks into hospital and steals computer containing private patient information	Required Encryption of Data

217. *See, e.g.*, Ornstein, *supra* note 36.

218. *See, e.g.*, *CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case*, *supra* note 95 (describing how CVS Pharmacy allegedly disposed of private health information in dumpsters accessible to the public).

219. *See, e.g.*, Thompson & Wohlsen, *supra* note 41.

C. Increasing Institutional Enforcement of HIPAA

1. Partnerships Between State Health Agencies and State Attorneys General

To better protect patient privacy, robust institutional enforcement of HIPAA is needed, which will require other agencies to assist OCR with HIPAA enforcement. OCR received nearly 13,000 HIPAA complaints in 2013.[220] Without additional funding and outside pressure to increase enforcement, OCR will continue to be overwhelmed by the volume of HIPAA complaints and respond by dismissing most complaints or seeking voluntary compliance from covered entities.[221]

A possible avenue for enhancing institutional enforcement of HIPAA lies in partnering state health agencies with AGs.[222] Shifting a portion of patient privacy complaints from OCR to a state health agency and AGs may help increase HIPAA enforcement. All fifty states have at least one health department that oversees a broad range of services that promote public health.[223] These state agencies may have familiarity with healthcare institutions within their state and knowledge of state and

220. *See Complaints Received by Calendar Year*, *supra* note 72. In addition to enforcing HIPAA, OCR is also responsible for protecting citizens from discrimination in certain social service and healthcare programs. *See Office for Civil Rights*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/office/index.html (last visited Sept. 26, 2014).

221. *See supra* Part I.C.

222. On January 16, 2014, the Federal Trade Commission (FTC) ruled that it may be able to file suit under HIPAA. *See* Order Denying Respondent LabMD's Motion to Dismiss, *In re* LabMD, Inc. (F.T.C. Jan. 16, 2014) (No. 9357), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (holding that the FTC may enforce HIPAA under section 5(a)(1) of the FTC Act, 15 U.S.C. § 45(a)(1) (2012), for a "company's failure to implement reasonable and appropriate data security measures"). While the FTC may emerge as a viable enforcer of HIPAA, it remains to be seen whether an appellate court will overturn the FTC's decision and how often the FTC will enforce the HIPAA Security Rule. Additionally, the Department of Justice tends to prosecute HIPAA violations under three specific circumstances: when patient records are stolen with the intent to (1) commit large-scale fraud, (2) commit financial fraud, or (3) embarrass the patient. Arriaza & Walsh, *supra* note 110. In these specific instances, the Department of Justice is likely to use a statute other than HIPAA for criminal prosecution. *Id.*; *cf.* Press Release, U.S. Att'y Office E. Dist. Tex., Former Hospital Employee Indicted for Criminal HIPAA Violations (July 3, 2014), *available at* http://www.justice.gov/usao/txe/News/2014/edtx-hippler-hipaa-kummerfield%20070314.html (describing the indictment of an employee of a covered entity who "obtained protected health information with the intent to use the information for personal gain").

223. *See, e.g.*, *State Health Departments and Services*, STATE & LOCAL GOV'T, http://www.statelocalgov.net/50states-health.cfm (listing state health departments). For example, the California Department of Public Health (CDPH) describes itself as "[d]edicated to optimizing the health and well-being of the people in California." *About Us*, CAL. DEP'T OF PUB. HEALTH, http://www.cdph.ca.gov/Pages/AboutUs.aspx (last visited Sept. 26, 2014).

federal privacy laws.[224] For example, the California Department of Public Health ("CDPH") investigated breaches of patient privacy and levied fines against several hospitals for violation of California privacy laws.[225]

A state legislature could require covered entities within its state to notify its patients that they can file privacy complaints not only with OCR, but also with the state health agency and the state AG.[226] The CDPH could continue to investigate and sanction hospitals for patient privacy breaches under state law, while also referring egregious violations to the California AG for possible charges under state law and HIPAA. Although partnerships between state health departments and AGs may significantly increase the volume of patient privacy complaints that AGs receive, this may help increase AGs' enforcement of HIPAA by: (1) encouraging AGs to shift their limited time and resources towards the increased volume of patient privacy complaints,[227] (2) aligning the number of patient privacy complaints

224. One example is the State of California Office of Health Information Integrity (CalOHII) which is empowered with "'statewide leadership, coordination, policy formation, direction and oversight for HIPAA implementation' . . . ." *Summary of CalOHII's Statutory Authority*, CAL. OFFICE OF HEALTH INFO. INTEGRITY, http://www.ohii.ca.gov/calohi/content.aspx?id=129 (last visited Sept. 26, 2014) (citing CAL. HEALTH & SAFETY CODE § 130303 (2012)).

225. *California Department of Public Health Issues Privacy Breach Fines to Five California Hospitals*, CAL. DEP'T OF PUB. HEALTH (June 10, 2010), http://www.cdph.ca.gov/Pages/NR10-039.aspx.

226. For example, section 130303 of the California Health & Safety Code provides that the California Office of HIPAA Implementation "shall assume statewide leadership, coordination, policy formulation, direction, and oversight responsibilities for HIPAA implementation. The office shall exercise full authority relative to state entities to establish policy, provide direction to state entities, monitor progress, and report on implementation efforts." CAL. HEALTH & SAFETY CODE § 130303. The California legislature could amend a provision like Section 130303 of the California Health & Safety Code (safeguards to protect privacy of patient information) to require covered entities within California to inform patients that the patients can file privacy complaints not only with OCR, but also with the CDPH and California AG. State health departments and AGs could also, at a minimum, list on their websites that residents can file complaints with either the health department or AG. The Tennessee Department of Health describes HIPAA on its website and directs consumers to file a complaint either with "the provider's Chief Privacy Officer" or OCR, leaving no mention of the Tennessee AG. *HIPAA: Health Insurance Portability and Accountability Act*, TENN. DEP'T OF HEALTH, http://health.state.tn.us/HIPAA/index.htm (last visited Sept. 26, 2014); *see supra* note 122 and accompanying text (describing the Illinois AG website which refers HIPAA complaints to OCR). Notifying state residents that they can file HIPAA privacy complaints with both a state health department and state AG would likely spread the volume of complaints among OCR, state health departments, and AGs. Because state health departments do not have the power to enforce HIPAA alone, the state health departments would need to work in conjunction with AGs or OCR.

227. This mitigates the concern of lack of time and resources among AGs as described in Part

AGs receive with HIPAA,[228] (3) allowing AGs to allege HIPAA as an additional cause of action when beneficial,[229] and (4) making patient privacy complaints seem like a worthwhile issue to address for political capital.[230]

State health departments, like AGs and OCR, face limited resources[231] and inconsistent privacy laws,[232] which may affect their abilities to help enforce HIPAA. State health departments, however, have existing relationships with covered entities and often devote a portion of their limited resources towards protecting patient privacy.[233] To address different state privacy laws, OCR may be able to allocate resources to training or informing state health departments on HIPAA Privacy and Security requirements like it did with AGs.[234] These partnerships have the potential to increase institutional enforcement of HIPAA and reduce OCR's workload.

A partnership of this type would likely address both willful and negligent breaches by increasing the amount and frequency of monetary penalties that a healthcare institution would face for HIPAA violations. Healthcare institutions may be inclined to implement more thorough security and training policies that would help control the behavior of their employees and minimize the likelihood of a negligent compromise of patient data. Because non-negligent breaches are generally out of the control of a covered entity, increased enforcement by a state health department–AG partnership may not deter non-negligent breaches.

II.B.1.

228. Addressing the concern that AGs use only federal statutes that align with the types of high volume complaints that they received as described in Part II.B.2.

229. While AGs may still choose to use exclusively state law causes of action, they may allege a HIPAA violation when HIPAA affords greater penalties as described in Part II.B.3.

230. Addressing the concern that AGs will not pursue cases that will not further their political careers as described in Part II.B.4.

231. Although state health departments may not suffer from most of the structural barriers that may prevent AGs from enforcing HIPAA, state health departments do face the challenge of limited time and resources. *See, e.g.*, Kim Krisberg, *Budget Cuts Straining Capacity of Public Health Departments: Services in Demand*, 40 NATION'S HEALTH 1 (2010) (describing state public health departments across the country facing budget cuts).

232. *See, e.g.*, Lawrence O. Gostin et al., *Informational Privacy and the Public's Health: The Model State Public Health Privacy Act*, 91 AM. J. PUB. HEALTH 1388, 1389 (2001).

233. *Id.* ("[S]tate public health agencies have an excellent track record of safeguarding public health data.").

234. *See* Anderson, *supra* note 110. OCR would have an incentive to train or inform state health agencies on the privacy floor set by HIPAA so that the health departments could help enforce HIPAA and reduce OCR's burden.

Healthcare institutions, however, may be able to mitigate the effects of non-negligent breaches through the complimentary security measures described below in Part III.D.1.

2. Limited Private Causes of Action?

HIPAA does not provide patients with private causes of action for privacy breaches.[235] Providing patients limited private rights of action to sue for damages under HIPAA may strengthen institutional enforcement of HIPAA.[236] While critics may contend that the healthcare industry is better regulated by federal agencies than private causes of action[237] or that OCR is likely to enforce HIPAA adequately in the future,[238] OCR does not have the proper resources to enforce HIPAA effectively. Providing a process for patients to submit their claims to an administrative body prior to filing suit will help mitigate concerns that a private right of action may cause more problems than it solves.[239]

Professors Sharona Hoffman and Andy Podgurski propose amending HIPAA to allow for a private cause of action, allowing patients to file

---

235. *See* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 337 (2007). While HIPAA has been successfully used to establish a standard of negligence in tort suits for breach of patient confidentiality, most courts do not accept HIPAA as a standard for negligence. *See* Brill, *supra* note 96, at 2120–24.

236. Although HIPAA does not provide a private right of action, some courts may allow a plaintiff to reference HIPAA in order to establish a standard of care in negligence suits. *See, e.g.*, I.S. v. Wash. Univ., No. 4:11CV235SNLJ, 2011 WL 2433585, at *2–5 (E.D. Mo. June 14, 2011) (declining to dismiss negligence *per se* claim based on HIPAA as standard of care and remanding to state court). Without private rights of action through HIPAA, victims of patient privacy breaches are turning to other causes of action. For example, in a class action lawsuit filed against AvMed for losing laptop computers containing PHI of 1.2 million patients, the plaintiffs filed suit under theories including negligence, breach of contract, breach of the implied covenant of good faith and fair dealing (referring to HIPAA regulations), and a Florida state law for misleading advertising. First Amended Complaint, Resnick v. AvMed, Inc., No. 1:10-cv-24513-JLK (S.D. Fla. Jan. 14, 2011). Other patients have resorted to common law and state law causes of action in lieu of HIPAA. *See Circumventing HIPAA's Absence of Private Right of Action*, PULSE (ACA Int'l Health Care Section, Minneapolis, Minn.), Dec. 2011, at 1, 3, *available at* http://socredit.com/wp-content/uploads/2012/01/Dec-2011.pdf.

237. *See generally* Abigail R. Moncrieff, *The Supreme Court's Assault on Litigation: Why (and how) it Might be Good for Health Law*, 90 B.U. L. REV. 2323 (2010).

238. *See* Brill, *supra* note 96, at 2118–20 (noting that since the HIPAA Privacy Rule first took effect in 2003, OCR has gradually increased the number of investigations and corrective actions that have been engaged in each year, which suggests that the agency has become more efficient with time).

239. *See id.* at 2130–38.

suit in federal court for breaches of patient privacy and recover actual damages (not less than $2500).[240] Their proposed HIPAA amendments would also allow plaintiffs to recover punitive damages for willful or reckless breaches and reasonable attorney's fees.[241] Arming individual patients with private causes of action may help deter patient privacy breaches with the threat of well-publicized litigation, help patients resolve their issues more efficiently than an overburdened federal agency, and help develop HIPAA rulemaking through judicial decisions.[242] Patients who are affected by a breach of privacy and are assisted by counsel would be motivated to enforce their rights under HIPAA and would not suffer from the same structural limitations faced by AGs as discussed in Part II.B.[243]

Amending HIPAA to allow a private right of action does not come without criticism. Professor Abigail Moncrieff contends that eliminating private rights of action in the healthcare industry is beneficial because federal agencies can better regulate the healthcare industry by using their expertise and economies of scale.[244] Moncrieff's argument has some merit and would translate to OCR's regulation of HIPAA.[245] As a federal agency, OCR possesses

---

240. Hoffman & Podgurski, *supra* note 235, at 383. Hoffman and Podurski would like to amend HIPAA to include:

> (a) Any person aggrieved by any act of a covered entity in violation of this section may bring a civil action in a United States District Court.
>
> (b) The court may award—
>
> (1) actual damages, but not less than liquidated damages in the amount of $2500;
>
> (2) punitive damages upon proof of willful or reckless disregard of the law;
>
> (3) reasonable attorney's fees and other litigation costs reasonably incurred; and
>
> (4) such other preliminary and equitable relief as the court determines to be appropriate.

Id.

241. *Id.*

242. *Id.* at 356.

243. While patients also have limited time and resources, they would likely be willing to allocate their time and resources to address egregious breaches of their patient privacy.

244. Professor Moncrieff states that federal agencies have greater institutional competency to regulate the healthcare industry than the courts because "generalist juries and judges are bad at understanding, evaluating, and creating healthcare regulations – and expert agencies might be much better. Furthermore, federal regulation of healthcare might make more sense than state regulation for a variety of reasons, especially considering the economies of scale that we gain from operating nation-wide." Moncrieff, *supra* note 237, at 2329–30.

245. Professor Moncrieff uses four examples of federal agencies in the healthcare field that could act as alternatives to private rights of action: Medicaid and the Center for Medicaid & Medicare Services (CMS), Employee Sponsored Insurance and the Department of Labor, Medical Devices and the Food and Drug Administration, and medical error and CMS/Professional

tremendous patient privacy expertise due to its role in processing tens of thousands of HIPAA complaints.[246]

Moncrieff admits, however, that the "biggest barrier to robust federal executive regulation right now is the agencies' shortage of resources for enforcing their statutes. To engage in robust regulation, the agencies need bigger staffs and more funding."[247] In theory, OCR could effectively enforce HIPAA with an unlimited budget by conducting thorough investigations of the thousands of complaints, but this is quite unlikely. OCR was budgeted only $41 million in 2011 and 2012, and its budget was reduced by $2 million and by ten full-time employees in 2013.[248] Given OCR's history of HIPAA enforcement, shrinking budget, and the increasing number of HIPAA complaints,[249] it will be very difficult for OCR to act effectively as an institutionally competent federal agency as envisioned by Moncrieff. While individuals may not possess the institutional expertise of a federal agency, these patients have the potential to actually enforce HIPAA by investing their own time and resources in litigation.

In allowing a private right of action under HIPAA, Congress should consider forcing plaintiffs to seek administrative adjudication prior to filing suit in order to filter weaker claims out of the judicial system.[250] Requiring prospective litigants to exhaust administrative remedies may help ensure that covered entities and business associates do not face a large volume of baseless claims and may help ease concerns that a private right of action will significantly increase the costs of maintaining HIPAA compliance.[251] Because OCR already conducts an intake and review of HIPAA complaints,[252] OCR could potentially serve as the administrative body that filters HIPAA complaints that fail

---

Associations. *Id.* at 2339–46.

246. *See Enforcement Highlights*, *supra* note 71.

247. Moncrieff, *supra* note 237, at 2380–81.

248. DEP'T OF HEALTH & HUMAN SERVS., FISCAL YEAR 2013: BUDGET IN BRIEF 108, *available at* https://web.archive.org/web/20131208155303/http://www.hhs.gov/budget/budget-brief-fy2013.pdf (last visited Sept. 26, 2014).

249. OCR received 12,915 HIPAA complaints in 2013. The second highest number of HIPAA complaints OCR has received in a year is 10,454. *See Complaints Received by Calendar Year*, *supra* note 72.

250. *See* Hoffman & Podgurski, *supra* note 235, at 384.

251. *See* Brill, *supra* note 96, at 2132 (warning that the costs associated with increased litigation would ultimately be passed along to patients).

252. *See Enforcement Process*, *supra* note 64.

to state a claim from the judicial system.[253] Like state agency–AG partnerships, private rights of action would likely address both willful and negligent breaches. The threat of HIPAA investigations and litigation by private parties may motivate covered entities to better implement and enforce security procedures. State agency–AG partnerships and considering limited private rights of action would strengthen the institutional enforcement of HIPAA.

D. Complementary Approaches to Institutional Enforcement

There is potential to strengthen the institutional enforcement of HIPAA through state health department–AG partnerships, private causes of action, or a combination of the two approaches. Complementing stronger institutional enforcement of HIPAA with additional security measures, such as requiring the encryption of data, conducting more audits without notice, and implementing some of the additional HITECH Amendments will better protect patient privacy against all three types of breaches described in Part III.B.

1. Requiring Encryption of Data

The American Medical Association describes data encryption as: "[T]ransforming information so that it becomes unreadable. This means that even if a hacker is able to gain access to a computer that contains PHI, he or she will not be able to read or interpret that information. The patient's privacy will still be protected."[254] The HIPAA Security Rule, however, does not require that covered entities encrypt patient data,

253. It is true that OCR may not have the proper resources to effectively review HIPAA complaints. *See* Hoffman & Podgurski, *supra* note 235, at 384 (noting that "[e]ffective administrative review, however, is dependent upon a strong network of agency offices that are adequately staffed to process a large volume of claims. HHS's anemic HIPAA enforcement record indicates that it does not currently have such resources."). Given that OCR already processes HIPAA complaints, however, it may make sense for OCR to act as the Equal Employment Opportunity Commission (EEOC) in the employment discrimination context and issue "right to sue" letters to individuals alleging HIPAA violations. *See* 42 U.S.C. § 2000e-5(f)(1) (2012) (stating that a plaintiff alleging employment discrimination based on Title VII of the Civil Rights Act of 1964 must obtain a "right to sue" letter from the EEOC prior to filing suit). OCR could continue to "resolve" HIPAA complaints that suffer from a procedural defect or fail to state a claim, thereby filtering a large number of suits from the judicial system. *See supra* note 65 and accompanying text.

254. *HIPAA Security Rule: Frequently Asked Questions Regarding Encryption of Personal Health Information*, AM. MED. ASS'N, http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf (last visited Sept. 26, 2014).

stating that encrypting PHI is "addressable" rather than "required."[255]

Congress should amend the HIPAA Security Rule to require covered entities and their business associates to encrypt patient data. While requiring additional time and resources, encrypting patient data can be done relatively easily and cost effectively.[256] The time and resources spent encrypting patient data will strengthen patient privacy protections, especially in cases of non-negligent breaches. In many data breaches, covered entities were victims of theft, resulting in the loss of millions of unencrypted patient records.[257] Had those hospitals encrypted their patient data, the thieves likely would have been unable to view the patient data in a meaningful manner.[258]

Healthcare institutions can also ensure that PHI stored on other devices at risk for theft, including computers, laptops, and USB drives, is encrypted. As an additional benefit, institutions that encrypt patient records would not be required to report breaches affecting more than 500 individuals to the media. Under section 13402(e)(2) of the HITECH Act, covered entities must provide notice to the media of breaches of "unsecured protected health information" affecting more than 500 individuals.[259] But, if a healthcare institution's patient records were secured through encryption, the institution would not be required to notify the media. Even if Congress does not amend the HIPAA Security Rule, it would be prudent for covered entities to seriously consider encryption to protect their patient data and save money in the event of a data breach.[260]

---

255. HIPAA Security Rule, 45 C.F.R. § 164.312(a)(2)(iv) (2013).

256. *HIPAA Security Rule: Frequently Asked Questions Regarding Encryption of Personal Health Information*, *supra* note 254, at 4–5 (explaining that after initially encrypting data "the process of encrypting and decrypting data should be virtually automatic," and that encryption does not have to be expensive).

257. Thompson & Wohlsen, *supra* note 41 (describing a computer stolen from Sutter Medical Center that contained unencrypted patient data); *see* Press Release, Office of Minn. Att'y Gen., Attorney General Swanson Sues Accretive Health for Patient Privacy Violation, *supra* note 108 (describing a laptop computer stolen from a car that contained unencrypted patient data).

258. *HIPAA Security Rule Frequently Asked Questions Regarding Encryption of Personal Health Information*, *supra* note 254, at 2 (describing how only those in possession of a "key" can unscramble the data to its original form).

259. HITECH Act § 13402(e)(2) (codified at 42 U.S.C. § 17932(e)(2) (2012)).

260. After the theft of an unencrypted device containing PHI, the chief security officer at the Alaska Department of Health and Social Services noted that his department would have saved millions of dollars in settlement and other costs if the department had encrypted its patient data. Marianne Kolbasuk McGee, *Inside a HIPAA Breach Investigation*, HEALTHCARE INFO SEC. (Sept. 12, 2012), http://www.healthcareinfosecurity.com/interviews/inside-hipaa-breach-investigation-i-1652.

Critics contend that encrypted data may still pose security risks.[261] For example, an employee could accidentally store the "key" used to unscramble encrypted data on the same computer that contains the patient data.[262] With access to the "key" on a stolen computer, a thief could unlock the encrypted patient data. To address this concern, the HIPAA Security Rule could require that covered entities store the encryption key on a separate device from the patient data. While it is true that covered entities may continue to face issues resulting from the theft of PHI even if their patient data is encrypted, requiring encryption will significantly mitigate the risk of harm resulting from stolen hardware containing patient data.

2. Modifying Audit Procedures

Congress could also require OCR to modify its audit procedures to (1) conduct HIPAA compliance audits without notice to the covered entity and (2) conduct more audits. These modifications to the audit process would complement the increased institutional enforcement of HIPAA by state health departments–AGs and private causes of action. OCR developed an audit program in 2011 to track the HIPAA compliance of covered entities.[263] These audits, however, are unlikely to be effective because "[e]ntities selected for an audit will be informed by OCR of their selection" before the auditors "interview key personnel and observe processes and operations to help determine compliance."[264]

First, implementing an audit system without advance notice will prevent covered entities from changing their day-to-day patient privacy protocols for the purposes of appearing HIPAA compliant during the audit. Without advanced notice, covered entities will be unable to alert their employees and modify their practices and procedures for the duration of the audit. OCR would not be unique in conducting site-visits without notice. The Centers for Medicare & Medicaid Services may conduct unannounced, on-site inspections to confirm compliance

---

261. *See, e.g.*, Amalia R. Miller & Catherine E. Tucker, *Encryption and the Loss of Patient Data*, 30 J. POL'Y ANALYSIS & MGMT. 534 (2011), *available at* http://dspace.mit.edu/handle/1721.1/75854#files-area.

262. *Id.* at 537.

263. *Health Information Privacy: HIPAA Privacy, Security, and Breach Notification Audit Program*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html (last visited Sept. 26, 2014).

264. *Health Information Privacy: Audit Pilot Program: How Will the Audit Program Work?*, DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html (last visited Sept. 26, 2014).

with its standards in certain instances.[265] Audits without notice will help address willful and negligent breaches by providing hospitals with an incentive to implement security policies in order to prepare for a potential upcoming audit.

Additionally, OCR should attempt to conduct more audits. In 2012, the audit program fell short of its 150 target audits,[266] and the chance that an individual institution will get audited is low. Increasing the number of audits may help OCR identify a greater number of covered entities in violation of HIPAA and allow OCR to bring the entities into compliance and prevent patient privacy breaches.[267] OCR may face budgeting issues in trying to implement an expanded audit process. If other agencies such as state health departments partnering with AGs enforce HIPAA more thoroughly, however, this may allow HHS to dedicate more of their limited resources towards conducting audits without notice.[268]

3. HITECH Amendment's Other Proposals

Although this Article illustrates that the HITECH Amendment allowing AGs to file suit under HIPAA will be ineffective, other portions of the HITECH Amendments may indeed better protect patient

---

265. *See* Independent Diagnostic Testing Facility, 42 C.F.R. § 410.33(g)(14) (2013) (noting that Independent Diagnostic Testing Facilities (IDTF) must permit CMS or its contractors "to conduct unannounced, on-site inspections to confirm the IDTF's compliance" with its standards for reimbursement).

266. *See* Agency Information Collection Activities; Submission to OMB for Review and Approval; Public Comment Request, 78 Fed. Reg. 32,389 (May 30, 2013) (soliciting feedback from the 115 covered entities audited by OCR in 2012); Howard Anderson, *Fewer Than 150 HIPAA Audits Expected*, HEALTHCARE INFO SEC. (Feb. 27, 2012), http://www.healthcareinfosecurity.com/interviews.php?interviewID=1407 (providing statements from an OCR official regarding the failure to reach the target number of audits).

267. Susan McAndrew, OCR's Deputy Director of Health Information Privacy, noted that the audit process allows OCR to bring "entities into compliance and highlight the importance of risk assessments." Patrick Ouellette, *OCR Provides New Security Auditing Enforcement Plans*, HEALTHIT SEC. (Dec. 5, 2013), http://healthitsecurity.com/2013/12/05/ocr-provides-new-security-auditing-enforcement-plans/.

268. OCR plans to survey up to 1200 covered entities in an effort to select entities for its next round of HIPAA audits. Agency Information Collection Activities; Proposed Collection; Public Comment Request, 79 Fed. Reg. 10,158, 10,158 (Feb. 24, 2014). While it remains to be seen whether OCR increases the number of audits it conducts, it appears that OCR recognizes value in proactively addressing HIPAA compliance through audits rather than through the complaint process. *See* Ouellette, *supra* note 267 ("With regard to security rule compliance, auditing is a significant tool and will be much more valuable than complaint-driven processes. . . . We think if we can get out in front of the process in an audit function, as opposed to just following complaints, that we can help everyone get ahead of the curve.").

privacy. For example, one of the HITECH Amendments applies HIPAA directly to business associates.[269] Prior to the HITECH Amendments, business associates were only liable for violations of HIPAA through contracts with the covered entity.[270] In suing Accretive Health, the Minnesota AG relied on this HITECH Amendment because Accretive Health was a business associate and not a covered entity.[271] The Minnesota AG would not have been able to sue Accretive Health under HIPAA absent the HITECH Amendment.

Other HITECH Amendments increase penalties for non-compliance[272] and require covered entities to notify the media for breaches involving 500 or more patients.[273] These additional measures provide some mechanisms for deterrence because hospitals may fear the greater monetary penalties and the negative publicity as a result of having to report their large breaches to the media and having their names posted on the OCR website.[274] The HITECH Amendments were certainly well intentioned with a goal to improve patient privacy and HIPAA compliance, and some of the Amendments may certainly improve patient privacy. Even though the HITECH Amendment allowing AGs to file suit under HIPAA is unlikely to be effective given the existing structural barriers, implementing the proposals in this Article may make it more likely that AGs prioritize patient privacy breaches and help enforce HIPAA.

CONCLUSION

HIPAA lacks strong institutional enforcement, and AGs alone are unlikely to support OCR in protecting patient privacy through HIPAA. While OCR may investigate high profile breaches that affect millions of patients, better protecting patient privacy in an increasingly digital healthcare environment can be achieved through a combination of stronger institutional enforcement and other complementary measures. The framework provided in this Article for evaluating different types of

269. Holloway & Fensholt, *supra* note 98, at 86. ("[T]he HIPAA privacy and security rules [now] *directly* apply to business associates.").

270. *Id.*

271. Minnesota Complaint, *supra* note 177, ¶ 12.

272. Holloway & Fensholt, *supra* note 98, at 87–88.

273. In the case of a breach of 500 or more individuals, the covered entity must notify HHS and "prominent media outlets serving the area," and HHS will list the covered entity's breach on the HHS website. *Id.* at 87.

274. *See Breaches Affecting 500 or More Individuals*, *supra* note 5.

patient privacy breaches will help provide context for evaluating the effectiveness of different solutions.

Partnering AGs with state health departments that are already familiar with local healthcare organizations may shift the number of HIPAA complaints away from OCR and towards state agencies. In turn, HIPAA complaints may become a salient issue that AGs find worthwhile to address with the help of state health agencies. These partnerships, along with limited private rights of action, may give HIPAA legitimate enforcement power that effectively deters patient privacy breaches. Combining enhanced institutional enforcement of HIPAA with complementary security measures such as required encryption of patient data, an increased number of unannounced audits, and the other HITECH Amendments will provide a significant boost in protecting patient privacy.

Although the proposed solutions will not eliminate patient privacy issues, they will certainly help increase institutional enforcement of HIPAA and better protect patients' privacy. Different privacy measures may need to be adopted in the future as technology and healthcare institutions evolve. Recognizing the different types of patient privacy breaches will help policymakers implement solutions that allow healthcare employees to benefit from EMRs, while providing maximum patient privacy.