UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30 | Issue 4 Article 2

Summer 2014

Uncle Sam Knows What's In Your Medicine Cabinet: The Security And Privacy Protection Of Health Records Under The HITECH Act, 30 J. Marshall J. Info. Tech. & Privacy L. 667 (2014)

Ranjit Janardhanan

UNCLE SAM KNOWS WHAT'S IN YOUR MEDICINE CABINET: THE SECURITY AND PRIVACY PROTECTION OF HEALTH RECORDS UNDER THE HITECH ACT

RANJIT JANARDHANAN*

I. INTRODUCTION

Your doctor, like many other businesses, has adopted storing all of your personal and medical information on computers and computer storage devices (e.g. USB flash drives,[1] portable external hard drives, laptops, etc.). Imagine one day your doctor loses one of these external

---

* Ranjit Janardhanan earned his Bachelor of Arts degree in Psychology from Alfred University in 2002 and a Master of Arts degree in Organizational Psychology from Columbia University in 2004. In 2009, the author earned a Master of Arts degree in Higher and Postsecondary Education from Columbia University, and a Juris Doctor degree from The John Marshall School of Law in 2012. The author is currently a practicing attorney in New York and would like to extend his sincerest thanks to Rajeswari, Govindan, and Sibu for their unwavering support, boundless love, and for the inspiration to excel by their living examples. Additionally, the author would also like to thank the JITPL editorial staff for their help bringing this Article to publication.

1. With the advances in technology, thousands of documents can be scanned and stored onto computer devices. *How Many Pages in a Gigabyte*, LEXISNEXIS 1, 1 (2007), *available at* http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf. In fact, a 128 GB USB flash drive, one of the largest capacity flash drives on the market can store approximately 8,292,096 Microsoft Word pages. *Id.* Alternatively, this device that can literally fit in the palm of your hand has the capacity to contain as much data as over sixty complete sets of the Encyclopedia Brittanica (thirty-two books per set; total volume pages: 32,640). *Encyclopedia Brittanica,* AMAZON, http://www.amazon.com/2010-Encyclopaedia-Britannica-Encyclopedia-editorial/dp/1593398379/ref=sr_1_1?s=books&ie=UTF8&qid=1358983653&sr=1-1&keywords=encyclopedia+britannica+final+edition (last visited June 5, 2014).

hard drives.[2] It had contained information such as your name, Social Security number, medical information, home address and phone number, results of medical tests, doctor notes, and credit card information. In addition, consider the fact that the hard drive could easily be used by anyone and that your doctor notified you six months after he lost it.

Imagine that your doctor notifies you that someone hacked into his computer network, encrypted thousands of medical records including yours under a new password that only the hacker knows, and informs you that the hacker is demanding a ransom for the password.[3] Your identity is stolen and $900,000 in merchandise, gambling, and telephone services is charged in your name.[4] You spend $100,000 in order to restore your identity and credit.[5]

Now, imagine even after all of this, people are still opening credit cards and bank accounts in your name.[6] Someone takes out three mortgages in your name, and as a result, you owe $600,000 in mortgage loans and another $100,000 in car loans and credit card debt.[7]

---

2. On or about October 2, 2009, fifty-seven unencrypted computer hard drives were stolen from a BlueCross BlueShield leased facility in Tennessee which included specific information for over one million people. *HHS settles HIPAA case with BCBST for $1.5 million*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Mar. 13, 2012), *available at* http://www.hhs.gov/news/press/2012pres/03/20120313a.html (noting that the drives contained protected health information (PHI) such as member names, Social Security numbers, diagnosis codes, dates of birth, and health plan identification numbers).

3. In June 2012, criminals hacked into the computer network of a small medical practice in northern Illinois, The Surgeons of Lake County, and encrypted the electronic medical records for thousands of patients. The criminals posted a message demanding a ransom payment in exchange for the password. Adam Levin, *For Ransom: Your Medical Records*, ABC NEWS (Aug. 22, 2012), http://abcnews.go.com/Business/ransom-medical-records/story?id=17051612; *see also Breaches Affecting 500 or More Individuals*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited June 5, 2014).

4. Jennifer Waters, *Identity Fraud Nightmare: One Man's Story Technology and the Recession Push ID Theft and Fraud to Record Levels*, MARKET WATCH (Feb. 10, 2010), http://www.marketwatch.com/story/the-rise-of-identity-theft-one-mans-nightmare-2010-02-10.

5. *Id*.

6. *Id*.

7. As a result of a free child scan for an identity theft protection service, a teenager learned that she owed $600,000 in mortgage loans and another $100,000 in car loans and credit card debt. Her Social Security number was stolen at the age of three and was used illegally to take out at least three mortgages, refinance mortgages two times, buy cars, and open at least forty-two credit card or charge accounts in her name. It was also discovered that eight different people used her Social Security number. Children's information can be stolen from numerous sources such as sophisticated cyber-attacks to simple theft of computers, school records, hospital records, or other physical equipment containing large amounts of child data. Ann Brenoff, *Teenager Owes $600,000 in Mortgage Loans After ID*

Or imagine that after your identity is stolen, and someone opens at least forty-two credit card or charge accounts, purchases cars, and refinances mortgages multiple times—all in your name.[8] These are all real life stories that happened to many people.

Does that concern you? Does it matter to you that because of the Internet, your personal, medical, and financial information could be sent to millions of people around the world? Fortunately, it matters to the United States government.

The United States government has taken steps toward strengthening America's economy and the general welfare of its citizens.[9] Congress passed the American Recovery and Reinvestment Act in 2009 ("ARRA") which served to revive America by expanding social welfare provisions, increasing unemployment benefits, implementing federal tax cuts, and directing increased funding to various areas such as education, infrastructure, and health care.[10] However, while increased funding and the creation of new programs within health care was premised upon helping Americans, its effect may not have been that limited.

At first glance, the substantial benefits of increased health care and newly designed electronic health record programs are very impressive. These programs yield benefits such as early identification and rapid response to public health threats and emergencies (such as bio-terror events and infectious disease outbreaks across the country), more accurate tracking of chronic disease management, reduced health care costs by significant administrative efficiency improvements, reduced medical errors, and decreased paperwork.[11] However, these benefits do not, by themselves, outweigh the significant threat of privacy breaches against many Americans.

There is significant potential for these programs to allow the federal government or more importantly, any person with access to the Internet, to misuse patient medical information. Misuse of patient medical information can subject many Americans to varying degrees of embarrassment, discrimination, and/or reluctance to seek out medical treatment. Unauthorized use can also subject numerous patients to

---

Theft, AOL REAL ESTATE (Oct. 14, 2011, 7:00 PM), http://realestate.aol.com/blog/2011/10/14/teenager-owes-600-000-in-mortgage-loans-after-id-theft/

8. *Id.*

9. American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, § 123 Stat. 115, 116 (2009).

10. Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 123 Stat. 226, 246 (2009) [hereinafter HITECH].

11. *Id.*

identity theft and substantial related costs. Costs may include remedying actual identity theft and/or future prevention of identity theft threats, once medical information was improperly accessed or stolen. In 2011, the total fraud amount was $18 billion,[12] which accounted for the total amount of funds the fraud operator obtained illegally. Additionally, identity theft victims must also endure months of emotional turmoil, loss of time, and frustration associated with resolving fraudulent activity with financial institutions and authorities.

Current legislation does not provide adequate assurances for preventing the misuse of medical information by the federal government or misuse by anyone with simple access to the Internet. Legislation pertaining to patient medical information includes the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[13] and the Health Information Technology for Economic and Clinical Health Act ("HITECH").[14] HIPAA provides guidelines for use of medical information by medical providers, medical clearinghouses, and by patients.[15] Additionally, the HITECH Act, a provision of the American Recovery Reinvestment Act, further establishes guidelines for any person creating, having, maintaining, or accessing patient electronic health records.[16] One of the original goals of HITECH was to have all patients' records converted entirely into electronic health records by the year 2014.[17] However, while many hospitals and medical offices have steadily converted to electronic health records, this goal has yet to be fully achieved.[18] From 2009 to 2012, electronic health record adoption has more than tripled among hospitals and nearly doubled among doctors.[19] Additionally, the U.S. government also aims to centralize patient

---

12. 2012 IDENTITY FRAUD REPORT: CONSUMERS TAKING CONTROL TO REDUCE THEIR RISK OF FRAUD, JAVELIN STRATEGY & RESEARCH 6 (Feb. 2012).

13. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 110 Stat. 1936 (1996) [hereinafter HIPAA].

14. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 246 (2009).

15. HIPPA, Pub. L. No. 104-191, § 110 Stat. 1936 (1996); *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. 2-3, 5-6 (May 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

16. § 123 Stat. at 259 (stating that "[t]he term 'electronic health record' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff").

17. 42 U.S.C. § 300jj–11 (2009); *see also Accelerating Electronic Health Records Adoption and Meaningful Use*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Aug. 5, 2010), *available at* http://www.hhs.gov/news/press/2010pres/08/20100805c.html.

18. Jacob Reider & Robert Tagalicod, *Progress on Adoption of Health Records*, HEALTH IT BUZZ (Dec. 6, 2013), http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/progress-adoption-electronic-health-records/.

19. *Id.*

information among and within states, providing for a nationally connected network of patient health information.[20] While collectively these goals seem to yield several benefits, storing large amounts of electronic patient medical information in one network is still very dangerous, since millions of patients may potentially fall victim to identity theft by cybercriminals[21] as well as fall victim to invasions of privacy. Furthermore, state and federal government agencies may also fail to continually secure the substantial amounts of personal information and this personal information may also be subject to unwarranted access by the federal government.

The centralization of this type of medical information along with the current inadequate security protocol for medical information collected by private health care providers, covered entities,[22] and other business associates[23] only invites potential breaches.[24] A "breach" is the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.[25]

---

20. *HITECH Priority Grants Program: State Health Information Exchange Cooperative Agreement Program*, U.S. DEP'T OF HEALTH & SERVS. (Aug. 2009), *available at* http://www.whitehouse.gov/assets/documents/HITECH_State_HIE_Cooperative_Agreement_Program_082009_(2).pdf; *see also* § 123 Stat. at 234.

21. On September 13, 2012, a foreign hacker stole 3.6 million Social Security numbers and 387,000 credit and debit card numbers from the South Carolina Department of Revenue. The foreign hacker methodically hacked the system on multiple occasions, which concluded with the last time on September 13, 2012—the date in which the actual theft of information occurred. The United States Secret Service collaborated in the investigation. Tim Smith, *Hacker Swipes 3.6M Social Security Numbers and other data*, USA TODAY (Oct. 26, 2012), http://www.usatoday.com/story/news/nation/2012/10/26/hacker-south-caroling-social-security-numbers/1660929/.

22. 45 C.F.R. § 160.103 (2013). Under the legislation, the term "covered entity" means:

> (1) health care plan; (2) health care clearinghouse; [and] (3) a health care provider who provides service who transmits any health information in electronic form in connection with a transaction covered by this subchapter. *Id.*

23. In general, a business associate is a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to or on behalf of a covered entity. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act, 78 Fed. Reg. 5566, 5688 (Jan. 25, 2013) [hereinafter Modifications].

24. *See* HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 258 (2009).

25. 78 Fed. Reg. at 5695 (defining a breach, in general, as the acquisition, access, use, or disclosure of protected health information in a manner that compromises the security or privacy of the protected health information. A breach does not include: 1) any unintentional access or use of protected health information by a person acting under the authority of a covered entity or business associate; 2) an inadvertent disclosure by an authorized user of protected health information to another authorized user of protected health information; 3) a disclosure of protected health information where a covered entity

This Article will discuss how the future centralization of health care information across the country and access by the U.S. government, despite substantial benefits and cost reduction, will pose substantial security and privacy threats to many Americans. This Article examines current legislation for creating, maintaining, and securing patient electronic health records and highlights the legislation's inadequacies in ensuring privacy now and without reform, in the future. Failure to reform current legislation will likely enable unauthorized users to easily access the nationally centralized information to embarrass, blackmail, or commit fraud against thousands, if not millions, of patients in the future.

Section II will discuss HITECH and its expansion of HIPAA. Section III will explore a variety of HITECH provisions, specific HIPAA provisions, and associated proposed reform. Provisions include breach notification, business associates and business associate agreements, enforcement and penalties, the minimum necessary rule, and centralization of information ramifications. Finally, Section IV will highlight the immediate need to draw attention to the HITECH Act and will also detail the potential consequences should future reform fail to take place.

II. BACKGROUND

Both HIPAA and the HITECH Act detail the legal requirements for creating, maintaining, and accessing patient medical information within the United States.[26] HIPAA outlines certain guidelines, which detail the necessary security provisions for which medical care providers are to follow when creating, maintaining, and accessing patient medical information.[27] Two sections of HIPAA outline these specifically: the HIPAA Security Rule[28] and the HIPAA Privacy Rule.[29]

---

or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information; and 4) any other acquisition, access, use, or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of various factors (nature and extent of the protected health information involved, the unauthorized person who accessed the protected health information, extent to which the risk to the protected health information has been mitigated)).

26. *The Health Information Technology for Economic and Clinical Health Act (HITECH Act)*, APA PRACTICE ORG. (Feb. 19, 2009), http://www.apapracticecentral.org/advocacy/technology/hitech-act.aspx.

27. *Health Information Privacy,* U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/index.html (last visited May 18, 2014).

28. *Health Information Privacy: HIPAA Security Rule*, U.S. DEP'T OF HEALTH &

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The HIPAA Security Rule requires certain physical, technical, and administrative safeguards to ensure the security, confidentiality, and integrity of electronically protected health information.[30] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, used, received, or maintained by a covered entity[31] and business associate.[32] In addition, covered entities and business associates must also: (i) identify and protect against reasonably anticipated threats to the security or integrity of information; (ii) protect against reasonably anticipated impermissible uses or disclosures; and (iii) ensure compliance by their own workforce.[33]

The Privacy Rule, another provision of HIPAA, requires safeguards to protect the privacy of protected health information,[34] and imposes limits and conditions on the uses and disclosures of such information that may be made without patient authorization.[35] The HIPAA Privacy Rule protects all "individually identifiable health information" or "protected health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[36] Protected health information includes demographic data that relates to: (i) an individual's past, present, future physical or mental health condition; (ii) the provision of health care to the individual; (iii) the past, present, future payment for the provision of health care to the individual; and (iv) and information that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual such as common identifiers such as name, address, birth date, and Social Security number.[37]

HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html (last visited May 18, 2014).

29. *Id.*

30. 45 C.F.R. § 164 (2013); *see also Health Information Privacy: HIPAA Security Rule, supra* note 28.

31. 45 C.F.R. § 160.103 (2010).

32. Modifications, 78 Fed. Reg. 5566, 5688 (Jan. 25, 2013); *see also* 45 C.F.R. §§ 164.304-318 (2009); *Health Information Privacy: HIPAA Security Rule, supra* note 28.

33. 78 Fed. Reg. at 5693; *Health Information Privacy: HIPAA Privacy Rule*, *supra* note 28.

34. 45 C.F.R. § 160.103 (2010).

35. 45 C.F.R. § 164.508 (2012); *see also Health Information Privacy: HIPAA Privacy Rule*, *supra* note 28.

36. 45 C.F.R. § 160.103 (2010).

37. *Id.* (stating that protected health information excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C.

The HIPAA Privacy Rule sets national standards to protect individuals' medical records and other personal health information and applies to health care providers that conduct certain health care transactions electronically, health plans, and health care clearinghouses.[38] The HIPAA Privacy Rule also gives patients rights to their health information, including rights to examine and obtain a copy of their health records, and to request corrections.[39] In addition, more recent federal legislation expands the security and privacy protocol for creating and maintaining patients' medical information in the form of electronic health records.[40]

B. HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

The HITECH Act further provides guidelines for any person creating, having, maintaining, or accessing patient electronic health records.[41] Electronic health records (EHR) are electronic records of health-related information about an individual that are created, gathered, managed, and consulted by authorized health care clinicians and staff.[42] Congress enacted the HITECH Act on February 17, 2009 for the purpose of creating a nationwide call for voluntary adoption of human information technology (HIT) throughout the entire health care system.[43]

The widespread use of HIT across the nation as well as local use can yield substantial benefits. Comprehensive management of medical information by centralization of information will improve the quality of health care, reduce costs through decreased paperwork and increased administrative efficiency, increase coordination among community resources, prevent medical errors, and will improve the continuity of care among health care settings.[44] These electronic health records

---

1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer).

38. *Id.* at §§ 160.102, 160.103; *see Summary of HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (last visited June 14, 2014).

39. *Id.*

40. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 231 (2009).

41. *Id.* at 260.

42. *Id.* (stating "[t]he term 'electronic health record' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff").

43. *Id.* at 230.

44. Tracy D. Gunter & Nicholas P. Terry, *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions*, 7 J. MED. INTERNET RES. 3, 5 (2005), *available at*

should include information such as recording vitals and demographics, summary of care records for transitions of medical care providers, clinical summaries for each physician visit, up to date problem list and current and active diagnoses, active allergy list, easy patient access to laboratory results, and active medication lists.[45] HIT will also allow for early detection of infectious diseases across the country and more accurate chronic disease management.[46]

Further, HIT can enable heath care providers to have ready access to patient information, which will expedite medical decisions and allow for health care providers to collect and calculate costs more efficiently.[47] This legislation reflects the government's substantial effort to establish a national electronic patient records system.[48] However, the HITECH Act was not the first step in attempting to do so.[49] Creating a national health care system in the United States has been an objective for some time now.

In April 2004, President George W. Bush issued an executive order to provide federal leadership in the development and national implementation of an interoperable electronic patient records system.[50] President Bush aspired to have every American have a personal electronic health record by 2014.[51] The order further established the Office of National Coordinator for Health Information Technology ("ONC") to direct and manage the evolution of HIT.[52] HIT involves the transformation of paper-based medical information into electronic health records using computer hardware and software.[53] The ONC also provides support to the National eHealth Collaborative, a federally recognized standards-setting body, which helps determine standards for providing privacy, security, interoperability, and other standards relating to electronic

---

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550638/; § 123 Stat. at 230.

45. Ravi Mariwalla, *Legislation Driven Transformation of U.S. Health care Delivery: Any Lessons for India?*, EXPRESS HEALTHCARE (Sept. 2010), http://www.expresshealthcare.in/201009/market37.shtml.

46. Gunter & Terry, *supra* note 44.

47. *The Health Information Technology for Economic and Clinical Health Act (HITECH Act)*, *supra* note 26.

48. *Id.*

49. *Id.*

50. Exec. Order No. 13335, 69 Fed. Reg. 84, 24059-60 (Apr. 30, 2004); *see also President Unveils Tech Initiatives for Energy, Health Care, Internet*, WHITE HOUSE (Apr. 26, 2004, 9:29 AM), http://georgewbush-whitehouse.archives.gov/news/releases/2004/04/20040426-6.html.

51. *President Unveils Tech Initiatives*, *supra* note 50.

52. Exec. Order No. 13335, 69 Fed. Reg. 84, 24059-60 (Apr. 30, 2004).

53. *The Health Information Technology for Economic and Clinical Health Act (HITECH Act)*, *supra* note 26.

health records.[54] However, since the enactment of the HITECH Act in February 2009, the ONC and HIPAA have taken on different roles and applications. The use of HIT has become more of an imperative and less of a recommendation.

Currently, the ONC is under oversight by the United States Department of Health and Human Services (HHS).[55] The ONC works to determine what HIT standards will be used and with HHS approval, coordinates efforts among federal agencies for expeditious implementation of HIT technology for use in the system.[56] Prior to implementation, HIT technology is reviewed for security and privacy compliance.[57] The government's objective of electronic health record centralization is primarily driven by the U.S. Department of Health and Human Services.

HHS is charged with providing grants to states to facilitate HIT technology and adoption of electronic patient records by providers.[58] HHS may provide qualified health care providers with HIT technology for a "nominal" fee, unless the HHS Secretary determines that their needs are already being met through the marketplace.[59] Factors such as the financial circumstances of smaller, low income or rural providers will also be considered before HIT technology distribution.[60]

HHS also offers assistance and guidance in helping health providers, insurers, employers, patients and other entities in understanding their rights and responsibilities related to federal privacy and security requirements related to electronic health records and rights regarding those records.[61] HHS provides a variety of methods to offers, incentives, grants, and loans to facilitate rapid implementation.[62] However, the government's substantial commitment to this centralization is not only marked by HHS oversight and its designated purpose for HIT implementation, but also by the new penalty scheme for patient security and privacy violations in addition to the other limitations for electronic health record use as set forth in the HITECH Act.[63]

---

54. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 241-42 (2009).

55. *The Health Information Technology for Economic and Clinical Health Act (HITECH Act)*, *supra* note 26; *About ONC*, HEALTHIT.GOV, http://www.healthit.gov/newsroom/about-onc (last visited June 14, 2014).

56. § 123 Stat. at 230-31.

57. *Id.*

58. *Id.* at 253.

59. *Id.* at 241.

60. *Id.*

61. *Id.* at 263.

62. *Id.* at 246.

63. Modifications, 78 Fed. Reg. 5566, 5583 (Jan. 25, 2013).

The HITECH Act mandates compliance beyond covered entities (public and private health care providers, health plans, and health care clearinghouses)[64] to their business associates.[65] Under HIPAA, federal legal requirements for maintaining, creating, and accessing patient medical information were generally limited to covered entities such as health care providers, health plans, and health care clearinghouses.[66] Health care clearinghouses are typically entities that assist health care providers or health plans with processing medical records.[67] Therefore, organizations such as regional health information organizations, e-prescribing gateways, and health information exchanges are now subject to HIPAA whenever these organizations conduct any work on behalf of providers, insurers, or other covered entities.[68] This new expansion under HITECH requires that any covered entity and business associate spanning the U.S. health care industry that utilizes or manages protected health information is required to comply.

Under the HITECH Act, both covered entities and business associates are required to notify a patient when his or her records have been breached.[69] This alerts patients who are victims of the breach and provides them with opportunity to mitigate potential harms.[70] Potential harms include identity theft resulting from the exposure of certain identifiers as well as reputational harm that might result from the exposure of sensitive medical information. The HITECH Act also mandates that breach notification regulations apply to vendors of health records as well.[71] Additionally, the new legislation further limits the ability of insurers, providers, or other entities to use patient information for marketing purposes and provides for more efficient enforcement and greater penalties for violation of privacy and security standards, including permitting HITECH enforcement through a state's attorney general's office.[72]

---

64. 45 C.F.R. § 160.103 (2010).

65. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 260, 264 (2009); Modifications, 78 Fed. Reg. 5566, 5570 (Jan. 25, 2013 (defining business associate).

66. *The Health Information Technology for Economic and Clinical Health Act (HITECH Act)*, *supra* note 26.

67. *Id.*

68. 78 Fed. Reg. at 5570.

69. The covered entity ultimately maintains the obligation to notify affected individuals of the breach under § 164.404. However, a covered entity is free to delegate the responsibility to the business associate that suffered the breach or to another of its business associates. This remains the case even if the breach of the covered entity's protected health information occurred at or by a business associate that is also a covered entity. *Id.*

70. *Id.* at 5682.

71. *Id.* at 5688.

72. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 274 (2009).

Prior to the HITECH Act, the HHS Secretary could impose a civil money penalty on any person who violated any section of HIPAA in an amount of not more than $100 for each violation, except that the total amount on the person for all violations of an identical requirement or prohibition could not exceed $25,000 during a calendar year.[73] Currently, the HITECH Act details a tiered penalty scheme where the HHS Secretary may levy more significant penalties as necessary by the nature and extent of the violation.[74] In contrast to the previous maximum penalty of $25,000, the current $1.5 million maximum penalty presents to be a more serious deterrent. Moreover, it more accurately reflects the importance of securing patient information.[75] During our current volatile economy, this maximum penalty amount would be difficult for any covered entity or business associate to endure.

A violation is timely corrected if the covered entity or business associate remedies the violation within a 30-day cure period.[76] The 30-day cure period for violations begins on the date that an entity first acquires actual or constructive knowledge of the violation.[77] The date will be determined based on evidence gathered by the Department of Health

---

73. Modifications, 78 Fed. Reg. 5566, 5682 (Jan. 25, 2013).

74. A Tier One violation is one in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision. The penalty amount is not less than $100 or more than $50,000 for each violation. In addition, a covered entity or business associate may be subject up to a $1,500,000 penalty for violations of the same requirement or prohibition in this category in a calendar year. *Id.* at 5683.

A Tier Two violation is one in which it is established that the violation was due to reasonable cause and not to willful neglect. Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision and was done without willful neglect. *Id.* at 5691. The penalty will be an amount not less than $1000 or more than $50,000 for each violation. *Id.* at 5583. The maximum penalty is $1,500,000 for violations of the same requirement or prohibition in this category in a calendar year.

A violation that is established to have been due to willful neglect and was timely corrected is considered a Tier Three violation. The penalty is an amount not less than $10,000 or more than $50,000 for each violation. The maximum penalty is $1,500,000 for violations of the same requirement or prohibition in this category in a calendar year. *Id.*

A Tier Four violation is a violation that is established to have been caused due to willful neglect and was not timely corrected. The penalty is an amount not less than $50,000 for each violation and the maximum penalty is $1,500,000 for violations of the same requirement or prohibition in this category in a calendar year. Under HITECH, covered entities and business associates may be subject to lesser penalties provided the violation is timely corrected. *Id.*

75. *Id.* at 5683.

76. *Id* at 5587.

77. *Id.*

and Human Services during its investigation, on a case-by-case basis. In addition, the Secretary of the Department of Health and Human Services is prohibited from imposing penalties for any violation that is timely corrected, as long as the violation is not due to willful neglect.[78]

In determining the amount of any civil money penalty, the Secretary will consider various factors, which may be mitigating or aggravating as appropriate.[79] Some factors include: (i) the nature and extent of the violation, such as the number of individuals affected and extent of physical or financial harm; (ii) whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance; (iii) how the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; (iv) the financial condition of the covered entity or business associate, consideration of which may include any financial difficulties that affected its ability to comply or whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; (v) the size of the covered entity or business associate; and (vi) such other matters as justice may require.[80]

C. HEALTH INFORMATION TECHNOLOGY IMPLEMENTATION PLAN

Overall health care objectives and health care policy priorities are tentatively set to be implemented in three stages. Beginning in 2011, Stage One included electronically capturing health information in a coded format to be used to track key clinical conditions and communicating that information for care coordination purposes.[81] Further, this information would be used in implementing clinical decision support tools to facilitate disease and medication management and reporting clinical quality measures and public health information.[82] Given the unanticipated rate of electronic health record technology adoption among hospitals and doctors' offices, the U.S. government had to revise

---

78. *Id.* at 5586.

79. *Id.* at 5691.

80. Modifications, 78 Fed. Reg. 5566, 5691 (Jan. 25, 2013).

81. *Meaningful Use Definition & Objectives*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives (last visited on June 5, 2014); Farzad Mostashari, *Stage 2 Meaningful Use NPRM Moves Toward Patient-Centered Care Through Wider Use of EHRs*, HEALTH IT BUZZ (Feb. 24, 2012, 4:48 PM), http://www.healthit.gov/buzz-blog/from-the-onc-desk/stage-2-meaningful-nprm/; *How to Attain Meaningful Use*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/how-attain-meaningful-use (last visited June 14, 2014).

82. *Meaningful Use Definition & Objectives*, *supra* note 81; Mostashari, *supra* note 81; *How to Attain Meaningful Use*, *supra* note 81.

the original timeline for the stages.[83] Stage Two will extend through 2016 and Stage Three will be effective in 2017.[84]

Stage Two will be effective in 2014 and will expand upon Stage One criteria to encourage the use of HIT for continuous quality improvement at the point of care and exchange of information in the most structured format possible.[85] Stage Two will primarily concentrate on more rigorous health information exchange, increased requirements for e-prescribing and incorporating lab results, and electronic transmission of patient care summaries across multiple settings including patient access to health records.[86] Stage Three will be effective in 2017 and will center mainly on promoting improvements in quality, safety, and efficiency—focusing on decision support for national high priority conditions and patient access to self management tools.[87]

Other government efforts under the HITECH Act have also contributed to widespread adoption of HIT. Under the American Recovery and Reinvestment Act in 2009 ("ARRA"), the HITECH Act amended Title XXX of the Public Health Service Act by adding Section 3013, State Grants to Promote Health Information Technology.[88] Under Section 3013, Congress established the State Health Information Exchange Cooperative Agreement Program.[89] Under this program, states and qualified State Designated Entities ("SDE") are awarded cooperative agreements to develop and advance mechanisms for information sharing across the health care system.[90] A cooperative agreement is a partnership between the grant recipient and the federal government. The State Health Information Exchange Cooperative Agreement Program

---

83. Reider & Tagalicod *supra* note 18.

84. Press Release, Ctrs. For Medicaid & Medicare Servs., CMS Rule to Help Providers make use of Certified EHR Technology (May 20, 2014), *available at* http://www.cms.gov/newsroom/mediareleasedatabase/press-releases/2014-press-releases-items/2014-05-20.html.

85. *Meaningful Use Definition & Objectives*, *supra* note 81; Mostashari, *supra* note 81; *How to Attain Meaningful Use*, *supra* note 81.

86. *Meaningful Use Definition & Objectives*, *supra* note 81; Mostashari, *supra* note 81.

87. *Meaningful Use Definition & Objectives*, *supra* note 81; Mostashari, *supra* note 81.

88. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 250 (2009).

89. PRASHILA DULLABH, ADIL MOIDUDDIN, CHRISTINE NYE, & LINDSAY VIROST, NORC AT UNIV. OF CHI., THE EVOLUTION OF THE STATE HEALTH INFORMATION EXCHANGE COOPERATIVE AGREEMENT PROGRAM: STATE PLANS TO ENABLE ROBUST HIE 1, 1 (Aug. 2011), http://www.healthit.gov/sites/default/files/pdf/state-health-info-exchange-program-evolution.pdf.

90. *State Information Exchange Programs*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange (last visited on June 5, 2014).

finances states' efforts to rapidly develop frameworks for exchanging health information across the health care system both within and across states.[91] Through this cooperative agreement, states will be awarded state grants to promote HIT.

The State Health Information Exchange Cooperative Agreement Program builds on existing efforts to promote both regional and state-level health information exchanges while advancing toward nationwide interoperability.[92] In March 2010, there were fifty-six grant recipients that included various states, eligible territories, and qualified SDEs.[93] As of January 2011, the U.S. government had provided $547,703,438 in grants to further the goal of interoperability of health information among and within states across the United States and various territories.[94]

America is in the age of technology. Information that was once stored in computers as large as vending machines can now be easily stored in devices that can simply fit in the palm of your hand. The centralization of patient electronic health records across the entire nation is an obtainable and almost certain goal. The utilization of such a centralized network of information has undeniable benefits which will have the overall effect of enhancing the interoperability, functionality, and utility of health care information.

Certified electronic health care records will provide health care providers with tools to reduce medical errors, improve patient care, and save on substantial costs of administrative processes, including less paperwork and more time-efficient medical processes.[95] Furthermore, centralization of electronic health records will facilitate early identification and rapid response to public health threats and emergencies such as bio-terror events and infectious disease outbreaks.[96] The benefits of this technology and its emerging implementation make this issue increasingly relevant. However, without further examination and necessary reform, the HITECH Act will not achieve its most basic purpose of protecting health information.

Close examination of current legislation will uncover certain vulnerabilities within the HITECH Act that renders it somewhat ineffective in preventing many unauthorized users from gaining access to protected health information. Once accessed, protected health information is susceptible to criminal misuse for blackmail, embarrassment, or

---

91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 235 (2009).
96. *Id. at* 230.

identity theft.

III. ANALYSIS

The HITECH Act substantially changes and extends the landscape of federal privacy and security law.[97] Specifically, the enactment of the HITECH Act results in the expansion of HIPAA and its Privacy and Security Rules which in effect, imposes increased breach notification protocol and requirements.[98] Breach notification requirements extend to covered entities and their business associates, provide for increased rights of individuals with respect to their patient health information,[99] provide for increased enforcement and penalties for violations, and permit certain limited uses and disclosures of protected health information.[100] However, while the HITECH Act significantly expands the enforcement power of HIPAA, it possesses significant vulnerabilities in areas of compliance and implementation.

The HITECH Act serves as the primary guideline for all medical professionals and business associates dealing with protected health information and securing electronic health information for the entire nation.[101] Therefore, the HITECH Act must address all threats to patients' privacy and security, especially with respect to patient electronic health records. However, under HITECH's present design, it does not do enough to enforce strict compliance or set out to protect millions of patients from identity theft. The following analysis is a review of the HITECH Act examining its strengths and highlighting other areas for

---

97. *Id. at* 226.

98. *The Health Information Technology for Economic and Clinical Health Act (HITECH Act)*, *supra* note 26; *see generally* Modifications, 78 Fed. Reg. 5566 (Jan. 25, 2013).

99. The HITECH Act requires that if an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. The covered entity is permitted to charge a fee for costs associated with labor and supplies for creating an electronic copy, including electronic portable media if agreed to by the individual and any postage if an individual requests that it be delivered by mail or courier. Modifications, 78 Fed. Reg. 5566, 5681 (Jan. 25, 2013).

100. 42 U.S.C.A. § 17931 (West) (stating "[S]ections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity"). Additionally, other security requirements within these regulations pertaining to covered entities are also applicable to business associates by way of business associate agreements between the business associate and covered entity. *Id.*

101. Modifications, 78 Fed. Reg. at 5566.

critical improvement.

A. BREACH NOTIFICATION

The HITECH Act is the principal federal law that imposes obligations upon covered entities and business associates for utilization of electronic health records.[102] The HITECH Act addresses and establishes clear and specific notification standards in the event of a breach of "unsecured patient health information."[103] "Unsecured patient health information" refers to protected health information ("PHI") that is not secured through the use of technology or methodology that renders PHI unusable, unreadable, or indecipherable to the unauthorized individuals.[104] "Secured PHI" consists of "unreadable" or "indecipherable" data and is not subject to the HITECH Act notification requirements.[105]

Encrypted data is data that has been encrypted with an algorithmic process that encodes the data in which a confidential and non-breached process or key is required to determine its meaning.[106] Destroyed data is data that is considered unusable, unreadable, or indecipherable which has been shredded or destroyed in a manner in which it cannot be reconstructed if in paper or hard copy form, or have been cleared, destroyed, or purged if the data was in the form of electronic media.[107]

Data stored on electronic media[108] must be destroyed in accordance

---

102. *Id.*

103. *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for information*, U.S. DEP'T OF HEALTH & HUMAN SERVS. 1-2, 4 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf (last visited June 5, 2014) [hereinafter *Guidance*].

104. *Id.*; Modifications, 78 Fed. Reg. at 5695.

105. *Guidance*, *supra* note 103, at 1-2, 5.

106. *Id.* at 16.

107. *Id.* at 17.

108. Electronic media means: (1) Electronic storage material where data may be recorded electronically such as devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media, such as the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately prior to the transmission. Modifications, 78 Fed. Reg. 5566, 5688 (Jan. 25, 2013).

with standards set by the National Institute of Standards and Technology ("NIST").[109] NIST is a non-regulatory federal agency within the U.S. Department of Commerce, whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.[110] When a breach occurs with unencrypted PHI, the HITECH Act imposes specific notification requirements to be followed for the party maintaining patients' electronic protected health information unless otherwise delegated by law.[111] A breach occurs when an unauthorized acquisition, access, use, or disclosure of protected health information that compromises the security and privacy of the information by an unauthorized person to whom the information is disclosed.[112] HITECH also imposes a significant extension of liability to business associates and business associates subcontractors for violations of protected health information and requires business associates to notify covered entities of any breach for which they are involved.[113]

The HITECH Act clearly defines what constitutes a breach and what does not. This provides a variety of practical and fiscal advantages which include: 1) cutting down on unnecessary paperwork (needless paper waste for patient notifications based on false breach determinations); 2) avoiding unnecessary costs associated with notification for covered entities; 3) decreased litigation; and 4) decreased investigations and associated investigative costs by the Department of Health and Human Services. Furthermore, the breach description within the HITECH Act not only provides for what constitutes a breach, but also details common scenarios involving protected health information that are not considered a breach.

Under HITECH, a breach does not include the unintentional access to PHI by an employee or other individual acting under the authority of a covered entity or business associate if the access was made in good faith, within the scope of employment or other professional relationship, and the information was not further acquired, accessed, used, or

---

109. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 231 (2009).

110. *NIST General Information*, NIST, U.S. DEP'T OF COMMERCE, http://www.nist.gov/public_affairs/general_information.cfm (last visited June 5, 2014).

111. § 123 Stat. at 261.

112. *See* Modifications, 78 Fed. Reg. at 5695.

113. Under the final rule, a business associate and business associate subcontractors are directly liable under the Privacy Rule for uses and disclosures of protected health information that are not in accord with its business associate agreement or the Privacy Rule. *Id.* at 5677. In addition, under the Security Rule, business associates are required to comply with many of the same requirements as covered entities, which in turn also subject them to the same penalties that apply to covered entities. *Id.*

disclosed by any person.[114] A breach also does not include the inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility, and the information "is not further acquired, accessed, used or disclosed without authorization.[115] Another exception to a breach under HITECH involves "a disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information."[116]

The clarity of this portion of the HITECH Act is practical and beneficial. It aids in avoiding unnecessary breach notifications and associated costs. Furthermore, it dispels any misconceptions on how easily HITECH can be violated since what constitutes a breach is clearly detailed. This should likely encourage more medical professionals to use HIT. Hospitals and doctors' offices often have electronic record networks that nurses and other staff have access to whether or not these nurses or personnel are assigned to these patients. Without such an exception for accidental access, these institutions would have to spend significant time and money for repeated breach notifications because this type of accidental access occurs repeatedly in many hospitals and office settings across the nation.

The HITECH Act also outlines specific timeframes and guidelines for notifying affected individuals.[117] Notification must be made "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach" by the covered entity or business associate.[118] However, breach notification may be delayed past sixty days if a law enforcement official requests a delay following a determination that such a notice or posting would impede a criminal investigation or cause damage to national security.[119] Both covered entities and business associates bear the burden of demonstrating that all notifications were made consistent with the timelines and notification specifications detailed by the ARRA.[120] The cap on making it no later than sixty days is a particularly effective provision of the HITECH Act.

---

114. Modifications, 78 Fed. Reg. 5566, 5695 (Jan. 25, 2013).
115. *Id.*
116. *Id*.
117. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 261 (2009).
118. *Id.*
119. *Id.* at 262.
120. *Id.* at 260-61.

Covered entities and business associates are compelled to investigate and resolve the breach and notification within sixty days.[121] Therefore, irrespective of how tedious or difficult an investigation into the breach might be, the breaching party is not permitted to notify affected patients beyond the 60-day period. Without the 60-day cap, covered entities and business associates would have little incentive to expedite the investigation since reporting the breach may subject them to a fine. Thus, they would likely adopt a more delayed investigative approach well past sixty days which would in turn, significantly delay providing any warning to affected individuals to be on alert for identity theft or other potential harm like blackmail.

A covered entity or business associate is obligated to provide notice once a breach is "discovered."[122] This obligation begins on the first day the breach becomes known or should have reasonably been known to the covered entity or business associate.[123] This obligation extends to "any person, other than the individual committing the breach that is an employee, officer, or other agent of such entity or associate."[124] Business associates are not obligated to notify the patient(s) of the breach directly, but are required to notify the covered entity of any and all breaches that occur.[125] Once the notification requirement is triggered, a covered entity must provide notice to the affected individual without unreasonable delay and in the manner prescribed by the HITECH Act.[126] Notice must be provided in writing and sent by first-class mail to the individual (or next of kin if the individual is deceased).[127] Notice may also be sent by e-mail should the patient prefer email correspondence.[128] Notice can also be provided by substitute form where there is insufficient evidence of the location of the individual.[129] The covered entity has two options for notification when there is a breach involving ten or more individuals for whom there is insufficient or out-of-date contact information.[130] First, it may provide a conspicuous posting on its website home page for a period to be determined by the Department of Health and Human Services.[131] Second, the covered

---

121. *Id.* at 261-62.
122. Modifications, 78 Fed. Reg. 5566, 5695 (Jan. 25, 2013).
123. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 260-61 (2009).
124. 78 Fed. Reg. at 5695.
125. § 123 Stat. at 260-61.
126. § 123 Stat. at 261; 78 Fed. Reg. at 5650.
127. § 123 Stat. at 261.
128. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 261 (2009).
129. *Id.*
130. *Id.*
131. *Id.*

entity may provide notice in major print or broadcast media.[132] This includes major media in the geographic regions where the individuals affected likely reside.[133] Additionally, for both options, a toll-free number should be included so individuals can learn whether their information was possibly compromised in the breach.[134]

The use of first class mail is an efficient method of notification since most people receive and read their mail. However, given the growing amounts of junk mail, there is a significant chance of this notification being discarded accidentally. Future reform should require a covered entity to both contact the individual by phone and use first class mail for every breach. Current substitute forms of notification by home page postings or broadcast media offer an easy and convenient method of notifying patients that a breach took place with respect to cost and immediacy of posting to a website. However, this efficiency and significant cost benefit is only advantageous to the breaching party and does little to ensure that victims of potential identity theft are actually notified.

Covered entities will likely bear little cost if any, to post this notification on their website. Furthermore, covered entities can gain access to their own home pages immediately with any piece of equipment that can gain access to the Internet. However, this notification method does have an added benefit. Posting a notification to a home page may incidentally inform potential patients who research medical practitioners via the web to be aware of health record breaches. This may serve as an additional deterrent since increased breaches may subject the medical practitioner to serious reputation ramifications. Patients will be less likely to seek out a medical practitioner or covered entity that has allowed patient protected health information to be breached. However, in urgent cases, the HITECH Act requires other notice methods to be employed.

In urgent cases where there is possible imminent misuse of unsecured PHI, covered entities may provide notice by telephone.[135] Further, if there is a breach, which affects more than 500 residents of a state or jurisdiction, covered entities are required to provide notice to "prominent media outlets serving a State or jurisdiction." In 2011, there were 250 breaches that involved 500 or more individuals.[136] As a result, more than 6,600,000 individuals were affected.[137]

---

132. *Id.*
133 *Id.*
134. Modifications, 78 Fed. Reg. 5566, 5651 (Jan. 25, 2013).
135. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 261 (2009).
136. 78 Fed. Reg. at 5671.
137. *Id.*

In addition, irrespective of the type of breach, all covered entities must notify HHS of any breach.[138] Actual notice to HHS is dependent upon the number of individuals affected. For example, in cases where less than 500 individuals are affected, the covered entity is only required to maintain a log of such breaches for annual submission to HHS.[139] In cases where a breach involved 500 or more individuals, the covered entity must provide a report to HHS immediately.[140]

Proposed reform should require that covered entities must submit a report to HHS for every breach of PHI within the 60-day limitation as set forth in the requirement for breaches involving 500 or more individuals.[141] This should be carried out in addition to the annual submission requirement and irrespective of the number of patients involved. Though submitting reports to HHS for every breach may pose to be a substantial administrative burden for HHS, it nonetheless provides a better chance for HHS to detect real problems with securing patient health information by covered entities that happen to experience breaches fairly regularly but inconspicuously. Current legislation may not uncover a significant security problem with a certain covered entity when breaches involving a small number of individuals occur sporadically and over time.

The lack of conspicuousness and sporadic timing may not trigger any alarms for HHS that a real security problem exists. Thus, the continual notification by a certain covered entity for each breach will, at the very least, give HHS more opportunities to become aware of a specific covered entity's potential security problems than one review of the covered entity's annual report.[142] In 2011, there were approximately 18,750 breaches that involved 500 individuals or less.[143] And because a breach involving less than 500 individuals was seventy-five times more likely to occur than a breach involving 500 or more individuals,[144] more attention should be required since the extensive financial harm and risk of identity theft to affected individuals can be equally substantial to those persons.

HITECH is intended to protect every individual, not just for breaches involving 500 or more individuals. The consequences of any

---

138. §123 Stat. at 262.

139. 78 Fed. Reg. at 5695; § 123 Stat. at 226.

140. *Id.* at 262.

141. *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/ (last visited Sept. 25, 2013).

142. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 262 (2009).

143. Modifications, 78 Fed. Reg. 5566, 5671 (Jan. 25, 2013).

144. *Id.*

breach, even one involving only a single person, can still be very serious for that one individual and should not be ignored. According to the Federal Trade Commission, identity theft and other scams cost Americans $1.52 billion dollars in 2011.[145] Every action that can prevent even one breach from occurring, irrespective of its potential administrative burdens, should be taken.

HHS must also submit a report to Congress detailing all breaches for which notice was provided to HHS annually.[146] Each report must include the total number of breaches across the nation, the nature of the breaches, and the actions taken in response to each breach.[147] According to a Department of Health and Human Services Annual Congress Report, from September 23, 2009 (data breach notification rule effective date) to December 31, 2010, there were approximately 7.8 million people affected by large data breaches of unsecured protected health information.[148]

The HITECH Act also mandates that certain information be included in the notice form.[149] The form of notice must contain, to the extent possible, the date of the breach, the date of discovery of the breach, a description of the breach, and a description of the types of unsecured PHI involved in the breach.[150] Additionally, it must also provide a description of the investigation into the breach, how the patient can mitigate losses, a description of what steps are being taken to protect

---

145. Kelly Phillips Erb, *How to Lose Your Identity in Five Easy Steps. Step One: Go to the Doctor*, FORBES (Oct. 21, 2013, 2:22 PM), http://www.forbes.com/sites/kellyphillipserb/2013/10/21/losing-your-identity-in-five-easy-steps-step-one-go-to-the-doctor/.

146. § 123 Stat. at 263.

147. *Id.*

148. From September 23, 2009 to December 31, 2009 covered entities notified approximately 2.4 million individuals affected by data breaches involving 500 or more individuals. From January 1, 2010 to December 31, 2010 there were approximately 5.4 million individuals affected by these large breaches. U.S. DEPT. OF HEALTH & HUMAN SERVS., ANNUAL REPORT TO CONGRESS ON HIPAA PRIVACY RULE AND SECURITY RULE COMPLIANCE FOR CALENDAR YEARS 2009 AND 2010 6, 10 (2010), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf [hereinafter U.S. DEP'T OF HEALTH & HUMAN SERVS. ANNUAL REPORT].

149. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 262 (2009).

150. *Id.* (stating that every notice of a breach will include: 1) a brief description of the breach detailing the date of the breach and date of discovery of breach, if known; 2) types of unsecured protected health information breached (e.g. name, Social Security Number, date of birth, disability code); 3) recommended steps for victims to prevent future harm from said breach; 4) a brief description of what the covered entity is doing to investigate the breach, mitigate losses, and to protect against any further breaches; and 5) contact information including a toll free number, Web site, and email address for any questions or concerns).

against further breaches, and the steps the individuals should take to protect them from potential harm arising from the breach.[151] The notice will also contain contact procedures for individuals to ask questions and obtain information. Contact information includes a toll-free phone number, email address, website, or postal address.[152]

Current notice requirements ensure that victims of the breach are sufficiently informed of all aspects of the breach. The notice requirements provide the victims of the breach with enough information to evaluate for themselves the danger of the breach and other additional information such as what steps are being taken to remedy the breach. While specific investigation details are generally not disclosed, the affected individuals are still given enough information to be able to follow up and take other mitigating actions should identity theft or other harms be a credible threat. No future reform is required for notice requirements once a breach is identified. However, unless a breach is recognized, the notice requirements and the tiered penalty system provide little to no benefit for providing any security or privacy for patients. This is a substantial flaw in the HITECH Act.

Even with clear notification requirements, once a breach is identified and a clear description of what penalties might be levied by HHS, the HITECH Act still affords covered entities and business associates too much latitude in identifying what constitutes a breach. The effectiveness of the HITECH Act relies heavily on covered entities and business associates to be forthcoming and proactive when identifying a breach. However, covered entities and business associates have little motivation to admit breaches or proactively identify a potential breach where one is not clearly apparent.

A party who must bear all costs in breach notification, who must conduct extensive investigation once a breach is identified and send notice within sixty days, who must implement new procedures to prevent future breaches,[153] and whose voluntary admission of the breach will likely result in fines outlined in the tiered penalty system,[154] is expected, under HITECH, to proactively and voluntarily admit to breaches. Recent cases highlight how attorney generals have sought remedy for compromised protected health information under HITECH and how delayed breach notification under state law has led to prosecution.

---

151. Modifications, 78 Fed. Reg. 5566, 5649 (Jan. 25, 2013).

152. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 123 Stat. 262 (2009).

153. *Id.*

154. 78 Fed. Reg. at 5583.

On January 13, 2010, in a lawsuit first of its kind in the nation,[155] the Connecticut Attorney General sued Health Net, Inc. for a massive security breach involving private medical records and financial information for more than 500,000 Connecticut citizens and 1.5 million consumers nationwide.[156] This is the first action by a state attorney general since HITECH newly authorized state attorney generals to enforce HIPAA violations.[157]

On or about May 14, 2009, Health Net, Inc. discovered that a portable computer disk drive containing Social Security numbers, protected health information, and bank account numbers disappeared from the company's office in Shelton, Connecticut.[158] The missing information included 27.7 million scanned pages of over 120 different types of documents.[159] These documents included correspondence and medical records, insurance claim forms, membership forms, and appeals and grievances.[160]

According to an investigative report by a computer forensic consulting firm hired by the defendant Health Net, the data was not encrypted or otherwise protected.[161] Therefore, any unauthorized person or third party could easily access the Social Security numbers, protected health information, and bank account numbers of approximately 2 million people that were contained on the computer disk drive through the use of commonly available software.[162] As a result of Health Net failing to encrypt this portable disk drive, the private and protected health information was left significantly vulnerable for criminal use. Moreover, Health Net also failed to promptly notify Connecticut residents whose personal information may have been compromised despite its own policies and requirements under federal law. Connecticut Attorney General Blumenthal alleged that Health Net failed to promptly notify his office or other Connecticut authorities of this missing protected health and other personal and private information.[163] Health Net's first notification action took place six months after discovery of the breach.[164]

---

155. *Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info*, CONN. ATT'Y GEN. OFF. (July 6, 2010), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

156. *Id.*

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*

163. *Id.*

164. *Id.*

It posted a notice on its website, and then sent letters to consumers on a rolling mailing basis beginning on November 30, 2009.[165]

The lawsuit alleged that Health Net failed to effectively supervise and train its workforce on policies and procedures concerning the appropriate maintenance, use, and disclosure of protected health information.[166] Blumenthal's lawsuit also named United Health Group Inc. and Oxford Health Plans LLC. Even though these companies did not cause the data breach, the companies were owners of Health Net of Connecticut.[167] This case highlights how even two of the largest medical insurance providers in the nation do not have the necessary protocols in place to prevent such breaches. Therefore, the threat of breaching patient health information is very real and unfortunately, too likely.

This substantial breach of patient health information was resolved by settlement among the parties. The settlement involves Health Net of the Northeast, Inc., Health Net of Connecticut Inc., and parent companies UnitedHealth Group Inc. and Oxford Health Plans.[168] In the settlement, Connecticut Attorney General Blumenthal negotiated stronger protections for individuals than what Health Net, Inc. initially offered, including two years of credit monitoring, $1 million of identity theft insurance, and reimbursement for the costs of security freezes.[169]

The settlement also provides powerful protections for consumers and a $250,000 payment to the state.[170] Blumenthal crafted a settlement that adequately addressed the entire spectrum of damages that this breach could potentially cause violated patients. This spectrum includes costs associated with credit monitoring and any identity theft costs that fall outside of covered liability but available with credit (e.g., credit cards, debit cards, creating new bank accounts, etc.). With contemplation of the delayed notification to state authorities, these added protections for victims of the breach were more necessary than convenient.

This case plays a unique role within the history of the HITECH Act. Given the date of the discovery for this breach, only certain HITECH provisions applied to this breach. For instance, HITECH newly authorized state attorney generals to enforce HIPAA violations that permitted the Connecticut Attorney General to sue Health Net under the HITECH Act. The Health Net breach was the very first action by a state attorney general aimed to enforce a HIPAA violation following the

---

165. *Id.*
166. *Id.*
167. *Id.*
168. *Id.*
169. *Id.*
170. *Id.*

enactment of the HITECH Act.[171] However, at the time, Health Net was not mandated to be in accordance with the breach notification rule under the HITECH Act when the breach took place; covered entities and business associates were not obligated to comply with breach notification obligations before the effective date (September 23, 2009).[172] Therefore, Health Net's first notification attempt six months after the breach discovery (on or about May 14, 2009) would normally be an added violation under the HITECH Act had the breach been discovered after the effective date.[173] Nonetheless, the six-month delayed notification illustrates how even one of the largest insurance companies can fail to appreciate the seriousness of compromising protected health information for patients. With the ease of disseminating information over the Internet, each day that goes by could mean an exponential increase in probability that victims of the breach will be financially exploited. In this case, the potential for financial exploitation increased over 180 days. [174]

Prompt notice to affected individuals allows these patients a fair opportunity to mitigate any losses. Affected individuals would have the opportunity to notify banks of potential fraudulent activity or, at the very least, get a warning that would encourage the affected individual to conduct a more careful review of any credit card or spending activity. The use of portable computer hard drives, and other computer technology, is widespread among the industry and accordingly, its associated risk of misuse is substantial.

In another case brought by the Indiana Attorney General, a large health insurance company, WellPoint, Inc., agreed to pay $100,000 for its failure to notify over 32,000 Indiana customers and the state of Indiana of a patient PHI breach.[175] The data breach occurred when applications for individual insurance policies were publicly accessible through an unsecured website from October 23, 2009 to March 8, 2010.[176] The breach ultimately affected approximately 645,000 individuals nationwide and involved Social Security numbers, customer credit card information, medical records, phone numbers, addresses, and other sensitive information.[177] This information was exposed online on

---

171. *Id.*

172. *HITECH Act Rulemaking and Implementation Update*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechblurb.html (last visited Sept. 25, 2013).

173. *Attorney General Announces Health Net Settlement*, *supra* note 155.

174. *Id.*

175. *Id.*

176. *Id.*

177. *Id.*

WellPoint, Inc.'s website for over 137 days.[178]

WellPoint, Inc. was made aware of the breach on February 22, 2010 but failed to notify any customers until June 18, 2010 (approximately four months later).[179] Under an Indiana state law (House Enrolled Act 1121-2009),[180] companies are required to notify both their consumers and the Attorney General "without unreasonable delay."[181] According to the Indiana Attorney General, "the requirement to notify the Attorney General 'without unreasonable delay' is not fulfilled by having me read about the breach in the newspaper."[182] News reports of the data breach ultimately prompted the Indiana Attorney General's Office to initiate contact to WellPoint on July 30, 2010 and launch an inquiry.[183] Therefore, the Attorney General was not officially involved until over five months after the breach was discovered.[184] To resolve the lawsuit, WellPoint agreed to conditions that include: to pay $100,000 to the state of Indiana, admit a security breach and failure to properly notify the Attorney General's Office, provide up to two years of credit monitoring and identity theft protection services for all consumers affected by the breach, and provide reimbursement to any WellPoint consumer of up to $50,000 for any losses that result from identity theft due to the breach.[185]

Both the Health Net and WellPoint cases demonstrate how companies have taken a relaxed attitude toward breach notification and how ramifications of such breaches go underappreciated. In both cases, the companies provided breach notification several months after the breach was discovered.[186] Both state attorney generals were able to obtain added credit monitoring and identity theft protection for victims of the breaches in their respective states that, as a result of delayed notification, was an absolute necessity. Despite being based on state law claims and being subject to different monetary penalties, lawsuits by attorney generals often share similar benefits as those brought under the HITECH Act.

Attorney generals litigating these violations help remove the cost factor for victims as the cost of litigation often deters victims from asserting their rights. Additionally, victims are more likely to report

---

178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.*
186. *Id.*

violations to state officials if actual justice for victims is repeatedly won. Furthermore, state action against covered entities and business associates also draws increased publicity and attention, which can serve as an additional deterrent for non-compliance.

Since electronic health record systems are self-regulated to the extent that covered entities and business associates must determine for themselves when a breach takes place, it is imperative that every possible deterrent be implemented to ensure breach notification actually takes place. Proposed reform for breach identification involves increased breach reporting submissions and additional proactive investigations by HHS. In addition to the annual submission requirement, covered entities and business associates should submit a detailed report to HHS for every breach. Increased submissions will cause more strict compliance by: (1) allowing HHS to more easily identify real security problems when breaches are being submitted more frequently from the same party; (2) serving as a fiscal deterrent because submissions will require additional work hours to complete at the various times in which a breach is discovered versus just compiling a list annually; and (3) increasing chances for repeated violators to be actually fined in accordance with the tiered penalty system.

Though submitting reports to HHS for every breach may pose a substantial administrative burden for HHS, the benefits substantially outweigh the costs. In addition, HHS should conduct more proactive investigations either randomly or through use of the increased submissions. Currently, HHS is developing a similarly intended investigative program called the HIPAA Privacy and Security Audit Program.[187]

Under Section 13411 of the HITECH Act, the Secretary is required to perform periodic audits to ensure HIPAA compliance.[188] In line with this requirement, in 2011, HHS initiated the pilot phase of this program called the Audit Pilot Program, where the Office for Civil Rights (OCR) engaged a professional public accounting firm (KPMG LLP) to conduct performance audits of various covered entities.[189] These audits enable OCR to ensure HIPAA compliance by close examination of a covered entity's and business associate's HIPAA privacy and security protocol.[190] In addition, the audits provide a new opportunity to identify

---

187. *HIPAA Privacy, Security, and Breach Notification Audit Program*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html (last visited June 5, 2014); *Audit Pilot Program,* U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html (last visited June 5, 2014).

188. *Id.*

189. *Id.*

190. *Audit Pilot Program, supra* note 187.

best practices and discover risks and vulnerabilities that may not have been obvious or apparent through OCR's ongoing complaint investigations and compliance reviews.[191] During the pilot phase of the audit program, OCR identified a pool of 115 covered entities for audits[192] which broadly represents the wide range of health care providers, health plans and health care clearinghouses operating today. According to OCR, business associates are also subject to audits but will not be audited until sometime in the future.[193]

These audits and other similarly intended proactive investigations could increase the chances of uncovering potential PHI breaches or alternatively, uncover actual breaches that have yet to be discovered or reported. Fear of an investigation will also serve as a surging motivator to comply. Additionally, future reform should also require that breaching parties provide credit monitoring services for each victim affected by the data breach. Similar in premise to both the Health Net[194] and WellPoint[195] cases where the attorney generals negotiated for two-year credit monitoring services for affected individuals,[196] the HITECH Act should also mandate that credit monitoring be offered by the breaching party for at least one year following discovery of the breach. Credit monitoring can very effectively minimize the disastrous effects of identity theft. It affords affected individuals an opportunity to at least contact the authorities and financial institutions (credit card companies, banks, etc.) to alert them to the fraud that is currently taken place so that the crime spree, identity theft, or other fraud can be halted in the beginning rather than weeks, and sometimes months, after when the significant damage has already been done. As another deterrent, breaching parties should also be mandated to publicize the total cost of corrective action in addition to the HHS fine on their business website and HHS's website for a period of one year (i.e., cost to covered entity or business associate for providing notice, labor costs for investigation, cost of credit monitoring services, newly implemented security encryption protocol). Non-breaching covered entities and business associates will be provided with actual costs for remediation for reference rather than mere estimation for what a data breach could actually cost.

This would serve as an added deterrent because other covered entities or business associates contemplating a loose security protocol would

---

191. *Id.*

192. *HIPAA Privacy, Security, and Breach Notification Audit Program*, *supra* note 187.

193. *Audit Pilot Program, supra* note 187.

194. *Attorney General Announces Health Net Settlement, supra* note 155.

195. *Id.*

196. *Id.*

reconsider once they actually became aware of actual cost data for remediating a breach. Ultimately, the cumulative cost of credit monitoring services and corrective actions for a breaching party will serve as an added deterrent for: (1) those covered entities and business associates who presently fail to appreciate the important nature of safeguarding this sensitive information and only value their own capital; and (2) to ensure that breaching parties moving forward will make every attempt to prevent future data breaches from occurring by implementing increased safeguards. It is an ongoing imperative that every action should be taken to avoid any breach of patient security and privacy. The consequences of such a breach for patients can be severe and should not be ignored.

B. BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

Prior to the HITECH Act, the provisions of HIPAA only applied to a business associate through a contractually created relationship with a covered entity.[197] As a result, remedies were severely limited. In the past, the only remedy available to a covered entity for a violation of HIPAA by a business associate was one of general contract law. Due to the enactment of the HITECH Act, business associates can now be directly liable for non-compliance.[198] Business associates currently have a direct legal obligation in both the application of the HIPAA requirements as well as with the penalties associated with a violation.

Under HITECH, a business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.[199] Some examples of a business associate include: (1) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information; (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity;[200] and (3) a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.[201] A subcontractor is a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.[202] A member of the covered entity's

197. Modifications, 78 Fed. Reg. 5566, 5667 (Jan. 25, 2013).
198. *Id.*
199. *Id.* (defining business associate).
200. *Id.*
201. *Id.* at 5573.
202. *Id.*

workforce is not a business associate.[203]

Business associates are required to comply directly with the HIPAA Security Rule's administrative, technical, and physical safeguard requirements.[204] Business associates and covered entities must create and document policies and procedures on how they will comply with the safeguard requirements.[205] Upon a breach of any of the security provisions, business associates are subject to the same potential civil and criminal penalties as covered entities.[206] This is a significant change in legislation as compared to that which existed prior to the HITECH Act. Previously, business associates were only bound to the terms and conditions detailed in the business associate agreement, rendering any remedy one of general contract law and nothing more. Business associates are now separately and directly liable for violations of the Security Rule and for violations of the Privacy Rule for impermissible uses and disclosures pursuant to their business associate contracts.[207] However, under the HITECH Act, business associates' obligations under the HIPAA Privacy Rule are not similar in extent to covered entities.

The HITECH Act obligates a business associate to use or to disclose protected health information consistent with its legal obligations as outlined in its business associate agreement with a covered entity.[208] More importantly, if a business associate violates the terms of its business associate agreement, it is subject to the same civil and criminal penalties under the HIPAA Privacy Rule for a covered entity.[209] Additionally, a business associate is directly liable for failing to disclose protected health information when required by the Secretary to do so in order for the Secretary to investigate and determine the business associate's compliance with the HIPAA Rules, and for failing to disclose protected health information to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of protected health information.[210] Business associates are also directly liable for failing to enter into business associate agreements with subcontractors

---

203. *Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last visited June 5, 2014).

204. Modifications, 78 Fed. Reg. 5566, 5677 (Jan. 25, 2013).

205. *Id.* at 5693.

206. *Id.* at 5677.

207. *Id.* at 5588.

208. *Id.* at 5691.

209. *Id.* at 5677.

210. Modifications, 78 Fed. Reg. 5566, 5591 (Jan. 25, 2013).

that create or receive protected health information on their behalf. [211]

This new expansion of liability is a considerable benefit for securing patient protected health information and a substantial strength for the HITECH Act. This will serve as a significant deterrent for those looking to gain unauthorized access or make unauthorized disclosure of PHI. Business associates have similar access to PHI and share a similar risk of unauthorized disclosure of PHI. This is an important change, particularly since prior to the HITECH Act, business associates did not bear any of the burdens of providing security and privacy unless specifically detailed in business agreements. This could be one of the strongest deterrents within the HITECH Act to prevent future harm to patients.

Business associates pose a significant threat to patient information with respect to unauthorized disclosure because business associates are sometimes individuals that are not intimately aware of HIPAA or the HITECH Act; often times, the inherent nature of their job as a business associate do not require them to be. Business associates include such positions as accountants, application services providers (supplying a full suite of information technology services including electronic health record and administrative systems), information technology implementation consultants, and lawyers.[212] Overall, the current business associate legislation is effective and the expansion of liability to business associates is a substantial safeguard to patient PHI. Future reform in this area is not required.

C. ENFORCEMENT AND PENALTIES

The HITECH Act expands civil penalties for HIPAA violations and imposes an additional formal investigation in specific instances. For example, enforcement is expanded in cases in which a violation of the HITECH Act is suspected to have been willful. In a case where a breach is willful, HHS is now required to conduct a formal investigation.[213] Furthermore, the HITECH Act also provides additional enforcement rights to state attorney generals who may prosecute civil actions in federal courts for their state residents affected by a HIPAA violation.[214] The HITECH Act further authorizes HHS to intervene in those actions.[215]

Under HITECH, civil and criminal penalties may be levied against covered entities and business associates for any violations associated

---

211. *Id.*
212. *Business Associates*, *supra* note 203.
213. 78 Fed. Reg. at 5578-79.
214. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 274 (2009).
215. *Id.* at 275.

with HIPAA and the HITECH Act.[216] Prior to the HITECH Act, the HHS Secretary could impose a civil money penalty for a HIPAA violation for an amount not more than $100 for each violation.[217] Furthermore, the maximum penalty could not exceed $25,000 during a calendar year for all violations of an identical requirement or prohibition.[218] Currently, the HITECH Act details a tiered penalty scheme where the HHS Secretary may levy more significant penalties such as a maximum penalty of $1,500,000 for a violation during a calendar year in any of the tiers as necessary by the nature and extent of the violation.[219] This applies to all violations of an identical requirement or prohibition during a calendar year.[220]

The tiered penalty system is a considerable strength for the HITECH Act and a necessary addition for HIPAA enforcement involving protected health information violations. It serves to impose significant penalties for breaches pursuant to the level of security and the degree of action on behalf of covered entities and business associates. The change in penalty amounts reflects the government's growing appreciation for the importance of securing this information and the associated costs of data breaches.

From a practical perspective, the tiered system affords HHS convenient latitude for litigation or remedy since breaches vary in degree and type. Some breaches may not fall exactly into one category or another, so the tiered penalty system allows for the factors that commonly impact court cases to be considered more easily and without injustice. Factors include cost of litigation, evidence of breach, and timeliness of lawsuit being litigated.

Overall, the HITECH Act has provided greater security and privacy through more stringent guidelines, which, by application, expands HIPAA's intended purpose of securing patient's health information from inappropriate use. Inappropriate use of this information can include embarrassing patients by publicizing past or current illnesses, using it for blackmail, or using it to commit identity theft. This tiered system serves as a clear deterrent for committing a breach, and alternatively promotes more efficient action to remedy a breach once a data breach is committed. No future reform is required in this area.

---

216. Modifications, 78 Fed. Reg. 5566, 5580 (Jan. 25, 2013).
217. *Id.* at 5582.
218. *Id.*
219. *Id.* at 5583.
220. *Id.*

D. MINIMUM NECESSARY STANDARD

Covered entities are required to use or disclose only the "minimum necessary" amount of PHI required to complete a covered function.[221] The Privacy Rule currently has in place a provision commonly referred to as the "Minimum Necessary Standard."[222] This standard requires that covered entities only disclose the minimum necessary amount of protected health information to accomplish the purpose of the permitted use or disclosure.[223] The HITECH Act has defined "minimum necessary" to be the use or disclosure of a limited data set, to the extent practicable, or if necessary, the minimum necessary to accomplish the intended purpose of the use or disclosure.[224]

Even though the Minimum Necessary Standard has a variety of exceptions[225] (such as an exception which permits disclosures or requests by a health care provider for treatment purposes), the government's future goal of a centralized network of patient health information will require a large network of business associates and covered entities to frequently contribute information for the ultimate well-being of patients. To meet this end, there will be thousands of employees accessing this centralized network just for computer maintenance and other administrative functions who will not be as knowledgeable as to what is minimally necessary for each medical situation.

Overall, the Minimum Necessary Standard is a good first step toward addressing the issue of using as little information as possible when exchanging patient protected health information. However,

---

221. "Minimum necessary" applies when using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. *Id.* at 5697.

222. Modifications, 78 Fed. Reg. 5566, 5645 (Jan. 25, 2013).

223. *Id.*

224. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 265 (2009); *see* 78 Fed. Reg. at 5697 (defining "minimum necessary").

225. The Minimum Necessary Standard does not apply to situations that involve: 1) disclosures to or requests by a health care provider for treatment purposes; 2) disclosures to the individual who is the subject of the information; 3) uses or disclosures made pursuant to an individual's authorization; 4) uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules; 5) disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes; and 6) uses or disclosures that are required by other law. *Minimum Necessary Requirement*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html (last visited June 5, 2014).

without establishing national standards or defining more clearly what satisfies the "minimal necessary information" requirement for the multitude of medical transactions, the millions of transactions utilizing the nationally centralized system will likely involve more than the necessary amount of protected health information being exchanged. As a result, these transactions will become thousands, if not millions, of opportunities for potential identity theft to occur.

The Minimum Necessary Standard provides a single benefit. It places both covered entities and business associates on notice that when engaging in any transaction, the extent of patient PHI should be considered carefully. However, the lack of any standard for what is considered "minimal" in relation to any particular transaction makes the benefits of this rule rather limited. Proposed reform should include a detailed list of what information is permitted for exchange during different types of transactions. Certain codes for medical procedures, tests, and prescriptions already exist for insurance purposes. Therefore, an expansion and national formalization of coding for medical procedures, prescriptions, and other medical testing may only be additionally required. It is important to balance the benefit of exchanging information efficiently with the significant risk for privacy breaches and criminal misuse.

E. CENTRALIZATION OF INFORMATION RAMIFICATIONS

HITECH will likely accomplish several of the primary objectives of informing clinical practice with the use of electronic health record ("HER") technology. Objectives include interconnecting clinicians so that health information can be exchanged using advanced and secure electronic communications, streamlining data collection, personalizing care with consumer-based health records and more up-to-date information for consumers, facilitating the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks, and improving public health through advanced bio-surveillance methods.[226] However, to make these objectives a certain reality, a centralized network of patient electronic protected health information would have to be created. And for a centralized network to excel, a large network of various covered entities and business associates would be required to participate. Thus, several thousands, if not millions of people, would need continual access to patient health information all around the country.

---

226. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 230 (2009).

Employees of covered entities and business associates would be responsible for adding or updating patient health information continually as medical procedures are performed, lab tests processed, X-ray, CT scan,[227] ultrasound or MRI[228] results received, and/or medications prescribed. However, while the benefits of such a system are undeniably substantial, the threat of potential identity theft is overwhelming.

Identity theft serves as a growing threat to all individuals within America. Given the increased digitization of information, globalization, and advanced use of the Internet within the United States and beyond its borders, "the environment is ripe with opportunities for identity thieves."[229] In 2010, 10.2 million Americans were victims of identity fraud.[230] In 2011, there were 11.6 million victims of identity fraud reflecting an estimated 1.4 million increase from the previous year.[231] The total fraud amount for 2011 was $18 billion,[232] which accounts for the total amount of funds the fraud operator obtained illegally; this may include actual losses to businesses or organizations and in some cases, consumers.[233] Additionally, there was a sixty-seven percent increase in the number of Americans impacted by data breaches compared to 2010, which is a likely factor for the increase in identity fraud from the previous year.[234]

These statistics indicate that identity theft presents a significant threat to many Americans. Identity theft is a growing concern because an increasing number of companies are collecting and storing personal information in their files that identifies customers and employees. While this information may be helpful for marketing, increase in sales, more speedy checkouts, and payroll, the failure to secure this information can result in identity theft, fraud, or other similar harms. Recent examples highlight how identity theft is a credible threat against patients and many Americans.

---

227. NAT'L INSTS. OF HEALTH, http://www.nlm.nih.gov/medlineplus/ency/article/003330.htm (last visited June 14, 2014) (discussing computer tomography scan).

228. *Id.* (discussing magnetic resonance imaging).

229. KRISTIN M. FINKLEA, CONG. RESEARCH SERV., R40599, IDENTITY THEFT: TRENDS AND ISSUES 1, 1 (2012), *available at* http://www.fas.org/sgp/crs/misc/R40599.pdf.

230. 2012 IDENTITY FRAUD REPORT: CONSUMERS TAKING CONTROL TO REDUCE THEIR RISK OF FRAUD, *supra* note 12.

231. *Id.*

232. *Id.*

233. *Id.*

234. *Identity Fraud Rose 13 Percent in 2011 According to New Javelin Strategy & Research Report*, JAVELIN STRATEGY & RESEARCH (Feb. 22, 2012), https://www.javelinstrategy.com/news/1314/92/Identity-Fraud-Rose-13-Percent-in-2011-According-to-New-Javelin-Strategy-Research-Report/d,pressRoomDetail.

In 2008, health and financial details of more than 2.1 million patients contained in computer files were stolen from a storage company hired by the University of Miami Health System.[235] During the same year, personal and health information for 6,000 patients was stolen from University of California, San Francisco and was available online for three months.[236] In January 2012, a laptop was stolen from the car of a Howard University Hospital contractor that contained protected health information for more than 3,400 patients.[237] Though password protected, the laptop contained personal information such as names, addresses, Social Security numbers, identification numbers, medical record numbers, birthdates, admission dates, diagnosis-related information and discharge dates.[238]

Other more recent examples draw increased attention to identity theft and the dangers of centralizing information particularly within government agencies. On March 31, 2011, it was discovered that names, addresses, Social Security numbers, dates of birth and driver's license numbers of 3.5 million Texans were accessible to the public because the Texas Comptroller's Office, a state governmental agency, failed to secure the information.[239] Records of 1.2 million Texans were transferred to this server in January 2010 and another 2 million records were transferred in April 2010, centralizing large amounts of personal information. According to the Texas Comptroller's Office, the personal information of 3.5 million Texans was unsecured "for a long period of time" and publicly accessible to any person with Internet access.[240]

In another case, on September 13, 2012, a foreign hacker had stolen 3.8 million[241] Social Security numbers, 387,000 credit and debit card

---

235. *Miami Patient Data Stolen*, AM. MED. NEWS (May 19, 2008), http://www.amednews.com/2008/05/19/bira0519.htm.

236. *Id.*

237. David Schultz, *As Patients' Records Go Digital, Theft and Hacking Problems Grow,* KAISER HEALTH NEWS (June 2, 2012), http://www.kaiserhealthnews.org/Stories/2012/June/04/electronic-health-records-theft-hacking.aspx.

238. Jeff Byers, *Stolen Laptop Affects 34K*, CLINCIAL INNOVATION+TECHNOLOGY (Apr. 2, 2012), http://www.clinical-innovation.com/topics/clinical-practice/stolen-laptop-affects-34k.

239. Kelley Shannon, *Breach in Texas Comptroller's Office Exposes 3.5 million Social Security Numbers, Birth Dates*, DALLAS MORNING NEWS (April 11, 2011), http://www.dallasnews.com/news/state/headlines/20110411-breach-in-texas-comptrollers-office-exposes-3.5-million-social-security-numbers-birth-dates.ece.

240. *Id.*

241. Robbie Brown, *South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere*, N.Y. TIMES (Nov. 20, 2012), http://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hackingepisode.ht

numbers, and 657,000 business tax filings[242] from the South Carolina Department of Revenue.[243] 16,000 of the credit and debit card numbers were unencrypted.[244] Additionally, none of the Social Security numbers were encrypted and therefore, could easily be used to commit millions of identity theft related crimes.[245]

State officials confirmed that the South Carolina Department of Revenue's website was hacked when an employee of the Department of Revenue opened a phishing email in August, giving the hacker access to the Department's data system.[246] During the ensuing weeks, the hacker patiently and systematically scoured the Department's system by remote access by utilizing the stolen employee's credentials and then finding more credentials once inside the system.[247] Over a two-day period in mid-September, the hacker zipped up huge data files and sent them to the Internet. Authorities discovered the theft on October 10, 2012. 74.7 gigabytes of data was stolen during this breach.[248] This is one of the largest computer breaches in the state or nation.[249] The United States Secret Service has joined the investigation.[250]

The significant potential of our personal information being misused is further highlighted in another example of a state government failing to adequately secure centralized information. On March 10, 2012, computer hackers illegally gained access to a Utah Department of Technology Services ("DTS") computer server that stores Medicaid and Children's Health Insurance Plan ("CHIP") claims data.[251] The hackers stole the Social Security numbers of 280,000 people along with other information for 500,000 people.[252] Other types of information stolen from the server may have included names, dates of birth, addresses, diagnosis codes, national provider identification numbers, provider taxpayer

---

ml?_r=0.

242. *Id.*

243. *Credit Protection for South Carolina Taxpayers*, S. CAROLINA DEP'T OF REV. (Oct. 24, 2013), http://www.sctax.org/security.htm.

244. Smith, *supra* note 21.

245. *Id.*

246. Tim Smith, *Security Gaps Still Exists 4 Months after S.C. Data Breach*, USA TODAY (May 20, 2013), http://www.usatoday.com/story/news/nation/2013/02/27/hacker-south-carolina/1951719/.

247. *Id.*

248. *Id.*

249. Smith, *supra* note 21.

250. *Id.*

251. *Common Questions*, UTAH DEP'T OF HEALTH, http://www.health.utah.gov/databreach/common-questions.html (last visited June 5, 2014).

252. *Id.*

identification numbers, and medical billing codes.[253] The hackers initially breached the server on March 10, 2012, but only began removing personal information when they breached the server the second time on March 30, 2012.[254] DTS detected the breach on April 2, 2012 and immediately shut down the server. Unfortunately, by that time, the information had already been stolen.[255]

Recent history has dictated that even a single theft at one location can threaten millions of patients and Americans. Therefore, the substantial threat of identity theft for millions of patients due to unauthorized access to a nationally centralized patient information network is not beyond imagination, but rather, a credible threat that has a limitless impact. Additionally, increased collection of personal information by various businesses for payroll, marketing, and/or billing has exacerbated the problem. Since more businesses collect such personal information, isolating where the identity theft actually occurred has become increasingly difficult to ascertain.

Consequently, this further limits the opportunity for identity theft victims to obtain adequate remedies for the breach since the party who failed to secure the information is not easily identifiable. Current legislation for identity theft and fraud may leave victims completely responsible for losses.[256] The lack of accuracy in isolating where a victim's information was stolen, the devastating damage identity theft can cause, and the limited legal remedies that exist for identity theft victims only increases the necessity for a more reformed HITECH Act which can ensure patient electronic PHI is properly safeguarded.

The HITECH Act has undeniably strengthened enforcement of penalties for patient PHI breaches and has expanded HIPAA's enforcement power. Prior to the HITECH Act, many have considered HIPAA

---

253. *Id.*

254. *Id.*

255. *Id.*

256. Victims of identity theft associated with debit card fraud may be responsible for the entire loss. Current legislation provides that timing of discovery of the fraud is indicative as to how much loss victims will be responsible for. If the discovery is within two days, victims are responsible for up to $50, and with anymore delay even up to $500. If identity theft is discovered more than sixty days without notice to the associated bank, the victim may be responsible for complete loss. In contrast, credit card legislation can be less complex and victims of identity theft are afforded more rights. *See* Karen Blumenthal, *Debit Cards: Think before You Swipe*, WALL STR. J. (Sept. 25, 2010), http://online.wsj.com/news/articles/SB10001424052748704062804575509812733666240; *Consumer Information: Lost or Stolen Credit, ATM, and Debit Cards*, FED. TRADE COMM., http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards#Limit (last visited June 5, 2014).

to be a weak enforcement scheme.[257] HIPAA penalties were limited to no more than $100 per violation and capped at $25,000 per year for all violations for identical types of breaches.[258] Even more, enforcement of these penalties generally took on an informal approach, as HHS and the Centers for Medicare and Medicaid Services (CMS) would investigate breaches without ever bringing formal charges.[259] HHS and CMS would work informally with the covered entity to accomplish compliance.[260] However, in the current climate and despite HHS' significant increase in authority to levy large fine amounts with the tiered penalty system, HHS is still fairly ineffective in preventing and penalizing data breaches by effect.

HHS' present record of imposing civil monetary penalties highlights its perceived ineffectiveness as a deterrent for future breaches. On February 4, 2011, HHS issued its first civil monetary penalty for a HIPAA violation.[261] It took HHS over seven years and 12,723 HIPAA Privacy Rule and Security Rule complaints where corrective action[262] was required before HHS imposed its first civil monetary penalty ever.[263] To understand the magnitude of complaints in terms of time, it would be as if one complaint was filed every day for over thirty-four years before HHS took action. While it can be noted that HHS has more recently been levying more penalties and entering more resolution

---

257. Norbert Kugele, *Hippa Goes Hitech: How The Hitech Amendments To Hippa Impact Employer-Sponsored Health Plans*, 35 MI TAX LAW. 19, 19 (2009).

258. Modifications, 78 Fed. Reg. 5566, 5582 (Jan. 25, 2013).

259. *Enforcement Rule – Final Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Feb. 16, 2006), http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enforcementfinalrule.html.

260. *Id.*

261. *HHS imposes a $4.3 Million Civil Money Penalty for Violations of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Feb. 22, 2011), http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html; *Case Examples and Resolution Agreements*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ (last visited June 5, 2014).

262. From April 14, 2003 (the HIPAA Privacy Rule Enforcement date) to December 31, 2010, there were 12,573 Privacy Rule complaints that resulted in corrective action. From April 20, 2005 (the Enforcement date of the HIPAA Security Rule) to December 31, 2010, there were more than 150 Security Rule violations requiring corrective action. Corrective actions taken by covered entities include: correcting any problems indicated by evidence in the investigation; training employees; sanctioning employees; revising policies and procedures; and mitigating any alleged harm. The goal of corrective actions is systemic change in the covered entity's policies and actions to ensure the proper protection of health information of individuals served by the entity. Only those complaints where violations were found and HHS found it necessary to take action were considered in the 12,723 calculation. U.S. DEP'T OF HEALTH & HUMAN SERVS. ANNUAL REPORT, *supra* note 148.

263. *Id.*

agreements[264] for HIPAA breaches, it cannot be denied that the increased frequency of fines is a likely reaction for the minimal enforcement during the previous several years. This is further supported by the increased number of resolution agreements.

A resolution agreement is a contract signed by HHS in which the covered entity agrees to perform certain obligations (e.g., staff training) and is required to submit reports to HHS (generally for a period of three years).[265] Resolution agreements are reserved to settle investigations with more serious outcomes and often require a payment of a resolution amount.[266] During the monitoring period, HHS will check the covered entity's compliance with its obligations.

Since April 14, 2003, the origin date of HIPAA Privacy Rule enforcement, to December 31, 2010, HHS has only entered into four (4) resolution agreements.[267] However, in 2011 and 2012, HHS has entered into seven resolution agreements. Therefore, HHS has nearly doubled the resolution agreements[268] in less than one-third the time (two years versus seven years) and in less than half complaints (5,988 versus 12,723)[269] where corrective action was ordered.[270]

Supporters of the HITECH Act are correct in their assessment that the HITECH Act markedly increases HIPAA's enforcement power. Unfortunately, this is not enough. The HITECH Act must be critically reformed to achieve its principal objective, assuring centralized electronic PHI is secured properly, and more specifically, less vulnerable to identity theft. This is paramount given the large amounts of personal and

---

264. 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 such period, HHS will monitor the covered entity's compliance with its obligations. A resolution agreement often includes the payment of a resolution amount. These agreements are reserved to settle investigations with more serious outcomes. However, when HHS has not been able to reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity. As of February 9, 2013, HHS has entered into eleven resolution agreements and issued CMPs to one covered entity. *Case Examples and Resolution Agreements*, *supra* note 261.

265. *Id.*

266. *Id.*

267. *Id.*

268. HHS entered into four resolution agreements for the previous seven-year period (April 14, 2003, the origin date of HIPAA Privacy Rule enforcement, to December 31, 2010). *Id.*

269. U.S. DEP'T OF HEALTH & HUMAN SERVS. ANNUAL REPORT, *supra* note 148.

270. *Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/ (last updated Apr. 30, 2014).

health information centralized in one computer network and its associated potential for serving as the "jackpot" for identity thieves.

Identity theft is a serious threat to many Americans. In 2011, the total fraud amount as a result of identity theft was $18 billion.[271] In addition, according to a final report issued in July 2012 by the U.S. Treasury Inspector General for Tax Administration ("TIGTA"), in 2011, there were approximately 1.5 million tax returns filed by identity thieves that went unidentified by the Internal Revenue Service ("IRS").[272] This ultimately costs the federal government, and, ultimately taxpayers, in excess of $5.2 billion in fraudulent tax refunds.[273] This was confirmed by the IRS.[274] Additionally, "the impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents."[275] The U.S. Treasury Inspector General estimates that identity theft will cause a total of $21 billion in potentially fraudulent tax refunds over the next five years.[276]

The potential "jackpot" of personal information, in addition to the ease in which it can be sent easily to millions of people by a simple click of a button over the Internet, makes the perils of identity theft involving the centralized network increasingly worse. The threat of having identity thieves utilize this centralized network of information for criminal means is real and potentially disastrous for many Americans.

This large network will be an endless reserve for identity thieves to easily access personal information for misuse or commit other types of fraud from multiple locations across the United States. This threat is even more apparent when considering recent incidents including: (1) a single theft of computer tapes from an employee's car that compromised the personal information (including Social Security numbers) of 4.9 million patients;[277] (2) in March 2011, the Texas Comptroller's Office, a

---

271. The total fraud amount is the total amount of funds the fraud operator obtained illegally. 2012 IDENTITY FRAUD REPORT: CONSUMERS TAKING CONTROL TO REDUCE THEIR RISK OF FRAUD, *supra* note 12.

272. *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting from Identity Theft*, TREAS. INSPECTOR GEN. FOR TAX ADMIN. (July 19, 2012), http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html.

273. *Id.*

274. *Id.*

275. *Id.*

276. *Id.*

277. On September 12, 2011, unencrypted back-up computer tapes for an electronic health record system were stolen from the car of an employee of a U.S. Department of Defense contractor. These computer tapes contained protected health information and personally identifiable information for over 4.9 million patients who received care from military facilities. Steve Vogel, *Tricare Military Beneficiaries Being Informed of Stolen*

state governmental agency, exposed the names, addresses, Social Security numbers, dates of birth and driver's license numbers for 3.5 million Texans on its website;[278] and (3) in September 2012, a hacker stole 3.8 million Social Security numbers as well as 387,000 credit and debit card numbers from the South Carolina Department of Revenue.[279] With these recent incidents in mind, one could only imagine how many people could be impacted if and when a nationally centralized system is compromised. In HITECH Act's current state and without further reform, identity theft will increasingly threaten many Americans.

F. PROPOSED CHANGES

Overall, the HITECH Act has several advantages. It lays out fairly clear notification requirements for all covered entities and business associates once a breach is actually determined.[280] Both covered entities and business associates should have little doubt as to what actions should be taken once a breach is discovered. More importantly, there is a clear description of what penalties they might face by HHS under the detailed tier penalty system outlined in the HITECH Act.[281] Furthermore, given the poor state of the economy, the increasing fines per type of breach will also serve to be a more effective deterrent than the previous penalty scheme. Business associates and other covered entities will likely be unable to endure such hefty fines, and thus, be more likely to strictly comply with the law. However, the HITECH Act still has one substantial flaw and, if not remediated, may undermine its very own purpose.

Electronic health record systems are self-regulated to the extent that covered entities and business associates must determine for themselves when a breach takes place. Under the present law, the breaching party who is: (1) responsible for paying the entire cost of notifying all of the patients associated with the breach; (2) required to complete an investigation to determine when and how the breach took place and bear associated costs; (3) responsible in later reforming the current procedures to prevent future breaches; and (4) required to notify the Department of Health and Human Services and likely be subject to

---

Personal Data, WASH. POST (Nov. 24, 2011), http://articles.washingtonpost.com/2011-11-24/politics/35283695_1_saic-personal-data-data-theft.

278. Shannon, *supra* note 239.

279. *Credit Protection for South Carolina Taxpayers*, *supra* note 243; Brown, *supra* note 241.

280. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, §§ 4001, 13001, § 123 Stat. 226, 226-79 (2009).

281. Modifications, 78 Fed. Reg. 5566, 5583 (Jan. 25, 2013).

monetary sanctions, is expected, under the HITECH Act, to voluntarily admit to breaches of protected health information.[282] If they do not recognize a breach, the tier penalty system and notification requirements are useless to protect the affected individuals since those are only triggered once a breach is identified. Simply, the U.S. government is almost wholly relying upon a party likely to be sanctioned to police themselves. Under the current scheme, covered entities and business associates have no real motivation to report breaches.

A violation of the HITECH Act will be difficult to ascertain by someone other than the covered entity or business associate. A violation of the HITECH Act generally requires a significant body of evidence, such as a stolen laptop or missing external hard drive that contained electronic patient health information. Moreover, the incidence of identity theft (the most significant effect of stolen PHI) is not, by itself, enough to alert patients that the breach took place at their doctor's office since personal and financial information is often collected by all types of merchants and various businesses.

This situation is further complicated because the U.S. Department of Health and Human Services ("HHS") has no idea whether a laptop or hard drive is ever stolen unless covered entities and/or business associates alert them. As a result, business associates and covered entities have great latitude in determining whether data breaches have taken place since they are not required to log all computers and hard drives containing electronic patient protected health information with HHS. Thus, when one goes missing, only the covered entity or business associate would know. Consequently, without such apparent evidence, it is very difficult to determine data breaches, and more importantly, it undermines the very purpose of the HITECH Act in securing patient information.

In HITECH's present form, the government expects a covered entity or business associate to voluntarily admit a breach much like how they would expect a murderer to voluntarily turn himself in when the police have no idea of his criminal culpability. This is strikingly similar to the tiered penalty system of the HITECH Act. Unless there is blatant evidence that can be discovered, there is no real incentive to admit a breach and even less incentive to voluntarily expose oneself to a substantial penalty. Three cases highlight both HIPAA and HITECH's significant vulnerability in data breach identification. In all three cases, HHS discovered breaches only after media reports highlighted the potential HITECH and HIPAA violations[283] that compromised protected

---

282. § 123 Stat. at 261-63; 78 Fed. Reg. at 5695.

283. These violations are deemed potential HIPAA violations only because no admis-

health information of millions of patients. It is undetermined whether HHS would have independently discovered these potential violations without the help of the media.

In one case that affected millions of consumers, several employees of CVS, the largest pharmacy chain in the United States with more than 6,300 retail outlets and online and mail-order pharmacy businesses,[284] were discovered discarding protected health information into dumpsters that were unsecured and easily accessible to the public. On January 16, 2009, CVS agreed to pay $2.25 million for the potential violation to the HIPAA Privacy Rule.[285]

The OCR[286] launched an investigation following media reports that alleged protected health information, maintained by several retail pharmacy chains, was being disposed of in dumpsters that were not secure and could be accessed by the public.[287] In addition to paying HHS, CVS Caremark Corporation, the parent company of the pharmacy chain, also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the Federal Trade Commission Act.[288]

On July 27, 2010, Rite Aid Corporation and its forty affiliated entities ("Rite Aid") agreed to pay $1 million to settle potential violations of the HIPAA Privacy Rule after television media videotaped incidents in which Rite Aid pharmacies were shown to have disposed of prescriptions and labeled pill bottles in open dumpsters easily accessible to the public.[289] These prescriptions and labeled pill bottles, that contained

---

sion of liability was included in the resolution agreements involving Rite Aid and CVS. However, in both cases, the parties agreed to pay large amounts of money ($2.25 million and $1 million, respectively) and agreed to undergo corrective action. *Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/riteaidresagr.html (last visited June 5, 2014); *Resolution Agreement: CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html (last visited June 5, 2014).

284. *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations,* FED. TRADE COMM. (Feb. 18, 2009), http://www.ftc.gov/opa/2009/02/cvs.shtm.

285. *Resolution Agreement: CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case, supra* note 283.

286. *OCR's Mission and Vision*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/office/about/mission-vision.html (last visited June 5, 2014).

287. U.S. DEP'T OF HEALTH & HUMAN SERVS. ANNUAL REPORT, *supra* note 148.

288. *CVS Caremark Settles FTC Charges*, *supra* note 284; *see* 15 U.S.C. §§ 41-58 (1914), *as amended*.

289. *Resolution Agreement*, U.S. DEP'T OF HEALTH & HUMAN SERVS. 2 (June 7, 2010),

individuals' protected health information, were being disposed of in various Rite Aid pharmacies across America.[290]

Rite Aid operates the third largest pharmacy chain in the United States, with about 4,900 retail pharmacies and an online pharmacy business.[291] Rite Aid is one of the nation's largest pharmacy chains and yet, with its extensive legal resources to ensure federal law compliance, it was the media that discovered the potentially serious HIPAA violations occurring across the country. Moreover, it was because of the media, and not fears of severe penalties or awareness of HIPAA laws, that OCR was able to prevent millions of patients from being victims of identity theft. In a separate but related action, the FTC also found Rite Aid to have violated federal law when employees of Rite Aid discarded consumers' personal information, such as pharmacy labels and job applications, in open dumpsters. The FTC investigation into Rite Aid also came following news reports.[292]

In another case, the OCR relied on media reports that indicated that computer backup tapes containing electronic PHI for two million individuals were stolen from a vehicle used by a hospital's off-site storage vendor.[293] Following the media reports, OCR initiated an investigation, which discovered gaps in the hospital's HIPAA Security Rule compliance program. As a result of the investigation, the hospital implemented a corrective action which included the adoption of encryption technologies on all backup tapes that contained electronic PHI, improvements to security awareness training policies, revision of the process for periodic review and updates of policies and procedures, and termination of the off-site storage contract and reevaluation of contractor requirements to transport and store backup tapes.

While the federal government has mandated increased security and privacy protocols, expanded liability to business associates, and markedly increased fine amounts, there is significant reform yet to be

---

available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/riteaidres.pdf.

290. *Id.*

291. *Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees*, FED. TRADE COMM. (July 27, 2010), http://ftc.gov/opa/2010/07/riteaid.shtm.

292. Rite Aid Corporation settled Federal Trade Commission charges that it failed to protect the sensitive financial and medical information of its customers and employees in violation of federal law. Under the settlement order, Rite Aid is required to establish a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from consumers and employees. In addition, Rite Aid is to undergo an audit every two years for the next twenty years from a qualified, independent, third party professional to ensure that its security program meets the standards of the order. *Id.*

293. U.S. DEP'T OF HEALTH & HUMAN SERVS. ANNUAL REPORT, *supra* note 148, at 15.

achieved. It is true that medical and business licenses may be at risk and significant monetary penalties might be levied for breaches that go unreported and later discovered by HHS. Nonetheless, this is still likely to be insufficient to outweigh the substantial cost of notification to alert victims affected by the breach, as well as the damage to the reputation of covered entities and business associates, once the information is released to the public. In many cases, covered entities and business associates may be risking more by reporting the breach than not.

By design, the HITECH Act is intended to be a reactive body of law that serves to act generally only when breaches are reported. Therefore, covered entities and business associates have better odds of not getting caught since the main trigger of the HITECH Act's notification and tiered penalty system begins with the covered entity or business associate admitting a breach.[294] Proposed reform should include HHS conducting more proactive investigations into select covered entities or business associates to uncover potential PHI breaches.

In addition, HHS should also require covered entities to submit a report to HHS for every breach of PHI within a reasonable period following each breach discovery, in addition to the annual submission requirement which will aid in narrowing the scope of investigations for HHS. This will allow HHS to detect and promptly correct real problems with securing patient health information by covered entities that happen to experience breaches fairly regularly but inconspicuously. Under the current legislation, HHS is less likely to identify a significant security problem with a certain covered entity when breaches involve a small number of individuals (under 500), which occur sporadically and over time. Additionally, HITECH should be amended to require that breaching parties provide credit monitoring services for at least one year for each victim affected by the data breach.

Credit monitoring provides victims a chance to at least contact the authorities and financial institutions to alert them to the actual fraud that is currently taken place so that the crime spree, identity theft, or other fraud can be halted prior to the criminal achieving maximum benefit of the theft. In addition, breaching parties should be required to post the total cost of corrective action in addition to the HHS fine on their business website and HHS's website for a period of one year. Such costs will include the cost to the covered entity or business associate for providing notice—cost for mailings, labor costs for investigation, cost of credit monitoring services, newly implemented security encryption protocol, etc.

---

294. Modifications, 78 Fed. Reg. 5566, 5580 (Jan. 25, 2013).

Covered entities or business associates will no longer have to imagine how much money they could stand to lose should a data breach take place. They will be provided with actual costs for remediation rather than estimation. Thus, this availability of reference will serve to encourage them to err on the side of more security than take the risk of paying the increased cost for remediation. Ultimately, this would serve as an added deterrent because other covered entities or business associates contemplating a loose security protocol would likely reconsider given the more definite costs of remediation for a data breach.

Even the potential cost of credit monitoring for victims of data breaches alone may serve as the necessary "push" that covered entities or business associates need to implement more secure protocols for PHI. For instance, in the South Carolina Department of Revenue case, where a hacker had stolen 3.8 million[295] Social Security numbers, 387,000 credit and debit card numbers, and 657,000 business tax filings[296] by accessing a government server, the State of South Carolina is paying approximately $12 million in credit monitoring service fees for one year for the estimated one million victims who signed up for credit monitoring.[297] The former South Carolina Department of Revenue Director, Jim Etter, told Senators that the password system (one protection method that would have greatly reduced the chance of the breach) would have cost only $25,000 to implement.[298] If the Governor of South Carolina was presented with an estimated cost of credit monitoring for potential victims, such as the $12 million, versus paying $25,000 for implementing password protection, the Governor would be more likely to elect the password protection by sheer financial calculation alone. While the benefit of hindsight is obvious, it still presents a situation where covered entities and business associates are more likely to implement security safeguards for electronic PHI for financial reasons alone.

Furthermore, increased publicity and prosecutions, as well as additional monetary penalties for failure to notify, will likely encourage covered entities and business associates to be forthcoming and proactive in handling data breaches. Since electronic health record systems are self-regulated to the extent that covered entities and business associates must determine for themselves when a breach takes place, it is imperative that every possible deterrent be implemented to ensure that breach notification actually takes place and patient information is ultimately

---

295. *Credit Protection for South Carolina Taxpayers*, supra note 243; Brown, *supra* note 241.

296. Brown, *supra* note 241.

297. Smith, *supra* note 246.

298. *Id.*

secured. Even though the HITECH Act is a considerable expansion of enforcement power for HIPAA, it is not, by itself, reason enough to not do more. The threat of misusing and losing electronic patient PHI is very real and highly likely. Recent cases highlight the real dangers that storing information electronically can pose and the necessity for HITECH.

On March 13, 2012, Blue Cross Blue Shield of Tennessee ("BCBST") agreed to pay HHS $1.5 million dollars as a result of the theft of fifty-seven unencrypted hard drives from a storage closet in 2009 that contained protected health information of over one million patients.[299] The hard drives contained personal information such as "names, Social Security numbers, dates of birth, diagnosis codes, and health plan identification numbers."[300] The hard drives were stolen from a data storage closet in a Blue Cross Blue Shield call center and were not password protected or encrypted.

According to OCR's investigation, BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes.[301] In addition, BCBST failed to implement appropriate physical safeguards by not having adequate facility access controls. According to HHS, the HIPPA Security Rule requires both of these safeguards.[302]

In February 2010, South Shore Hospital, a leading regional health care provider to 725,000 residents of Southeastern Massachusetts,[303] lost unencrypted back-up computer tapes that included names, Social Security numbers, financial account numbers, and medical diagnoses of more than 800,000 consumers.[304] South Shore Hospital shipped three boxes, containing 473 unencrypted back-up tapes, to Archive Data Solutions in Texas to be erased and resold. However, only one box arrived at the location. In May 2012, South Shore Hospital agreed to pay $750,000 to resolve allegations by the Massachusetts's Attorney General that it failed to protect the personal and protected health information of more than 800,000 consumers.[305] The lawsuit was filed under

---

299. *HHS settles HIPAA case with BCBST for $1.5 million*, *supra* note 2.

300. *Id.*

301. *Id.*

302. *Id.*

303. *About Us*, S. SHORE HOSP., http://www.southshorehospital.org/aboutus (last visited June 5, 2014).

304. Martha Coakley, *South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations*, ATT'Y GEN. OF MASS. (May 24, 2012), http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breachsettlement.html.

305. *Id.*

the Massachusetts Consumer Protection Act and the federal Health Insurance Portability and Accountability Act. The missing tapes have yet to be recovered.[306]

On September 12, 2011, unencrypted backup computer tapes for an electronic health record system were stolen from the car of an employee of Science Applications International Corporation, a U.S. Department of Defense contractor.[307] These computer tapes contained protected health information and personally identifiable information for over 4.9 million patients who received care from military facilities. The tapes contained personal information such as names, Social Security numbers, addresses, diagnoses, treatment information, provider names, provider locations and other patient information.[308] This data breach affected millions of patients across ten states: Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, Oklahoma, South Carolina, Tennessee and Texas.[309] This single theft at one location immensely threatened the financial safety and emotional well-being of millions of people across the country.

These recent cases highlight how protected health information such as names, Social Security numbers, addresses, and dates of birth can easily fall into the hands of identity thieves. Current use and rapid adoption of electronic health record technology across the nation makes this not only a pressing issue but poses imminent problems that require immediate attention and subsequent solutions. The consequences of a single data breach can be quite disastrous and recent history has shown it can even impact millions of people across multiple states. Thus, every attempt to make PHI more secure should not be easily ignored and should be more carefully considered.

The government should take every action that can prevent even a single data breach from occurring, irrespective of its potential administrative burdens. This is critically important since identity theft is rampant. Identity theft victims also face tremendous difficulty isolating the source of the data breach, which makes liability and appropriate redress almost impossible to obtain. Since an increasing number of

---

306. South Shore Hospital failed to even confirm that Archive Data had sufficient safeguards in place to protect this sensitive information. South Shore also neglected to inform Archive Data that personal information and protected health information was on the back-up computer tapes. Multiple companies handled the shipping of the boxes containing the tapes. *Id.*

307. Vogel, *supra* note 277.

308. *Id.*

309. Sig Christenson, *Data Breach Exposes 4.9 Million TRICARE Patients*, MY SAN ANTONIO (Sept. 29, 2011), http://www.mysanantonio.com/news/military/article/Tricare-patient-data-exposed-2194067.php.

merchants and various other types of businesses collect and store the same type of personal and financial information for marketing and other business purposes, it would be very difficult to prove where the identity thief stole the information. Presently, the effectiveness of the HITECH Act relies almost entirely on covered entities and business associates recognizing their own breaches. If they do not recognize a breach, the tiered penalty system and notification requirements are useless to protect the affected individuals.

IV. CONCLUSION

Centralization of electronic health records across the entire country is an obtainable and certain goal. The federal government has extended great efforts to lay out plans, in stages, for implementation of electronic health record technology by all hospitals, doctors, health care providers, and business associates.[310] Congress has tied standards, implementation specifications, and certification criteria to the incentives available under the Medicare and Medicaid EHR Incentive Programs when they utilize EHR technology in a meaningful manner.[311]

The federal government has even promoted increased digitization of patient health information through deterrence. For example, those physicians and hospitals that have not adopted EHR technology by 2015 will be assessed financial penalties in the form of lower Medicare fee reimbursement.[312] The rapid implementation of electronic health records and subsequent centralization is certain to occur and is undeniably beneficial.

Centralization will provide for more accurate tracking of chronic disease management, reduced medical errors, early detection of infectious diseases across the nation, reduced health care costs by significant administrative efficiency improvements, and decreased paperwork protocols.[313] Certified electronic health record technology will offer capabilities that can assist any health care provider to improve the quality, safety, and efficiency of the care they deliver.[314]

---

310. *Meaningful Use Regulations*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/meaningful-use (last visited on June 5, 2014).

311. *Id.*; American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001, § 123 Stat. 226, 246 (2009).

312. *Frequently Asked Questions: Are There Penalties for Providers Who Don't Switch to Electronic Health Record (EHR) Technology?*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/faqs/are-there-penalties-providers-who-don%E2%80%99t-switch-electronic-health-record (last visited June 5, 2014).

313. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001, 123 Stat. 226, 230 (2009).

314. HITECH, Pub. L. No. 111-5, § 123 Stat. 226, 230 (2009).

EHR technology will be the future of medical care. However despite the apparent benefits, the use and centralization of this information can, and likely will, put protected health information of millions of patients at terrible risk. A call for immediate reform for increased security protocol for electronic PHI and better rights for identity theft victims is required.

According to a Department of Health and Human Services Annual Congress Report, there were approximately 7.8 million people affected by large data breaches of unsecured protected health information from September 23, 2009 (data breach notification rule effective date) to December 31, 2010.[315] In 2011, there were 11.6 million people who were victims of identity fraud crimes.[316] In fact, according to the latest U.S. Census Bureau statistics, there were more victims of identity fraud in 2011 than there are people presently living in New York City.[317]

In addition, the costs associated with identity theft and identity fraud makes this problem a significant issue. The total amount of funds obtained illegally due to identity theft and other related fraud crimes in 2011 totals approximately $18 billion.[318] It is clear that identity theft and other fraud related crimes pose a serious threat to many Americans. The HITECH Act stands to be one of the best safeguards patients have for ensuring they do not fall victim to identity thieves. However, in its current form, the HITECH Act has certain vulnerabilities and is in need of immediate reform.

Future reform should include: HHS conducting more proactive investigations or significantly increasing audits into select covered entities or business associates to uncover potential PHI breaches, increased publicity and prosecutions to deter delayed notification, additional stiff monetary penalties for failure to notify HHS or patients, mandating credit monitoring services for affected individuals, and publicizing the total cost of corrective action, in addition to the fine imposed by HHS, on the covered entity's and HHS's websites for a period of one year, increased reporting of breaches at time of breach for all breaches irrespective of the number of individuals affected, and providing a more detailed list of what information is permitted for exchange during

---

315. U.S. DEP'T OF HEALTH & HUMAN SERVS. ANNUAL REPORT, *supra* note 148.

316. 2012 IDENTITY FRAUD REPORT: CONSUMERS TAKING CONTROL TO REDUCE THEIR RISK OF FRAUD, *supra* note 12.

317. According to the latest U.S. Census Bureau data, as of 2013, there are approximately 8.4 million people living in New York City. *New York (city), New York*, U.S. CENSUS BUREAU, http://quickfacts.census.gov/qfd/states/36/3651000.html (last visited June 14, 2014).

318. 2012 IDENTITY FRAUD REPORT: CONSUMERS TAKING CONTROL TO REDUCE THEIR RISK OF FRAUD, *supra* note 12.

different types of transactions for business associates and covered entities. Without such reform, the national centralization of this information will be an endless reserve for identity thieves to access personal, health, and financial information of millions of patients from multiple locations across the United States.

As a result, more resources will be allocated into investigations, increasing amounts of identity thefts will occur, patients will be subjected to humiliation or embarrassment, and there will be a substantial loss of time and financial resources for victims and their families seeking justice for these HITECH Act violations. Future reform is further necessitated because more and more businesses collect and store personal and financial information on computer devices, which makes isolating the source of the data breach tremendously difficult to identify. This in turn makes imposing proper liability and achieving appropriate redress for identity theft victims almost impossible to obtain.

In its present form, the HITECH Act will stand to secure some patient electronic PHI but will ultimately fail as the primary motivator for covered entities and business associates alike to make protecting patient health information a necessary priority. This will, in time, make the centralization of PHI more difficult and vulnerable for substantial misuse.