5-1-2013

The Inadequacy of the Damages Assessed Upon Violation of the Breach Notification Rule

Jeffrey David Gaskill

The Inadequacy of the Damages Assessed Upon Violation of the Breach Notification Rule

JEFFREY GASKILL

INTRODUCTION

As the world becomes increasingly digitalized, the importance of the security and privacy of client information rises as well. Congress has acknowledged this issue with the passage and proposals of various bills such as: The Privacy Act of 1974, the Gramm-Leach-Biley Act, the Personal Data Privacy and Security Act of 2011, the Personal Data Protection and Breach Accountability Act of 2011, and the SAFE Data Act.[1] "Information security laws are designed to protect personally identifiable information from compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or other situations where unauthorized persons have access or potential access to such information for unauthorized purposes."[2] However, despite statutory provisions and penalties designed to protect the public against the disclosure of personal health information, there have been about 55,500 instances of unsecured health information breach since 2009, with nearly 500 hundred of which having affected 500 or more individuals.[3]

This paper examines the Breach Notification Rule under the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Part I introduces a few cases of recent health data breaches that illustrate a need for stronger statutory provisions. Part II briefly discusses the legislative history of the Breach Notification Rule and looks to the pertinent statutory text. Part III looks at common causes of data breach and associated costs related to data

[1] GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 2 (2012).
[2] GINA STEVENS, CONG. RESEARCH SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 2 (2010).
[3] Lucas Mearian, *'Wall of Shame' exposes 21M medical record breaches*, COMPUTERWORLD (Aug. 7, 2012, 6:00 AM), http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches.

breaches. Part IV details what covered entities should be doing to ensure that they are compliant with pre-breach best practices and how to properly handle breaches once they occur. Part V outlines the current causes of actions that can be brought by either the Secretary of the Department of Health and Human Services or state attorney generals. Part VI examines some of the current, pending class action lawsuits that have been filed under state law privacy statutes and how a private cause of action would benefit the Breach Notification Rule. Finally, Part VII introduces suggested statutory amendments, partially drawn from state law and other areas of health, which should help to reduce the number of and severity of future health data breaches.

I. THE NEED FOR STATUTORY REVISIONS TO THE BREACH NOTIFICATION RULE

Congress has taken admirable steps in attempting to ensure the privacy of patient health records through the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH); a section of the American Recovery and Reinvestment Act which amended and added to the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Unfortunately, the Breach Notification Rule of the HITECH Act has been difficult for the Department of Health and Human Services (HHS) to finalize, partly because of the every-changing dynamic of the health information technology field and a large response to a call for public comment on the interim Breach Notification Rule.[4] Acknowledging the complexity of the issues at hand, HHS has withdrawn a developed final rule from the Office of Management and

[4] *Breach Notification Final Rule Update*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html (last visited Dec. 6, 2012). A contributing factor was the passage of the Affordable Care Act which has increased the speed in which health records are being converted to electronic medium. *See also Your Health and Your Privacy: Protecting Heath Information in a Digital World: Hearing Before the Subcomm. On Privacy, Technology, and the Law*, 112th Cong. (2011), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=9b6937d5e931a0b792d258d9b332c04d.

Budget "to allow for further consideration."[5] Given the number of breaches that have invoked the notification requirement and the subjectively lenient treatment thereof, the interim breach notification rule is insufficient as a means of deterrence against the wrongful disclosure of unsecure health information and the protection of patient privacy.[6]

The disclosure of patient-identifiable health records is an issue worthy of significant protection because patients maintain a fundamental right to privacy[7] (encompassing things like medical diagnoses, use of prescription medication, etc.) and more importantly, from a fiscal-sense, disclosure may place patients in danger of identity theft.[8] It is for these reasons that particular instances of health data breach are so frightening and why the Breach Notification Rule and resulting penalties must be tailored as a proper deterrence. The following two examples illustrate how breaches can transpire and will be useful in reading the rest of this paper.

A. The University of Miami Hospital Breach

In July 2012, law enforcement officers discovered that two University of Miami Hospital employees had been stealing patient "face sheets," containing "names, addresses, dates of birth, insurance policy numbers and reasons for the visit."[9] There is a possibility that the employees had sold the data to a third party and were immediately discharged from employment.[10] The

[5] *Breach Notification Final Rule Update*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html (last visited Dec. 6, 2012).
[6] *Breach Affecting 500 or More Individuals*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES: HEALTH INFORMATION PRIVACY, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Dec. 6, 2012).
[7] *See generally* Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890) (distinguishing a right to privacy under theories of life, liberty and property).
[8] *See generally About Identity Theft*, FIGHTING BACK AGAINST IDENTITY THEFT, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Dec. 6, 2012) (discussing the nature of identity theft, how it is committed, and how the information can be used).
[9] Alicia Caramenico, *U of Miami Hospital suffers patient data breach*, FIERCE HEALTHCARE (Sept. 12, 2012), http://www.fiercehealthcare.com/story/u-miami-hospital-suffers-patient-data-breach/2012-09-12.
[10] Dan Snyder, *University of Miami Hospital Data Incident: July 2012: Frequently Asked Questions*, UNIVERSITY OF MIAMI HOSPITAL, http://www.umhdataincident.med.miami.edu/ (last visited Dec. 6, 2012); Using patient

malfeasance allegedly occurred over a 22-month period beginning in October 2010 and affected thousands of patients, though an exact total is unknown.[11] While the "face sheets" did not contain financial information, Social Security Numbers were used as the insurance policy number for Medicare and Medicaid patients.[12]

Law enforcement delayed notification to the public in order to conduct a criminal investigation, as permitted by the Breach Notification Rule.[13] In compliance with the statute, the hospital sent a letter to affected individuals in September 2012 detailing the breach.[14] In addition, the hospital stated that it would review its practices to protect against future incidents and also offered two years of credit monitoring to affected individuals.[15]

The University of Miami Hospital breach is illustrative of several aspects of the Breach Notification Rule, many of which are discussed in detail *infra*. First, the hospital's lack of sufficient records kept them from gauging the scope of the breach. This surely increased the cost of providing credit monitoring since there were few parameters as to who it was offered to. Second, the involvement of law enforcement officials will likely result in criminal charges against the employees, but the fact that law enforcement discovered the breach could be indicative of the hospital having not complied with various security regulations. Finally, given that the actions of the hospital *employees* went undiscovered for so long, it is even more

---

information with the intent to sell is punishable with a fine of not more than $250,000 and/or imprisonment of not more than 10 years. 42 USCA § 1320d-6(b)(3) (West).

[11] John Dorschner, *Two University of Miami Hospital employees may have stolen, sold patient data*, THE MIAMI HERALD (Sept. 7, 2012), http://www.miamiherald.com/2012/09/07/2990379/two-university-of-miami-hospital.html.

[12] Erin McCann, *Miami hospital data breach due to employee offense*, HEALTHCARE IT NEWS (Sept. 11, 2012), http://www.healthcareitnews.com/news/u-miami-data-breach-due-employee-offense.

[13] Dan Snyder, *University of Miami Hospital Data Incident: July 2012: Frequently Asked Questions*, UNIVERSITY OF MIAMI HOSPITAL, http://www.umhdataincident.med.miami.edu/ (last visited Dec. 6, 2012); 42 USCA § 17932(g) (West).

[14] Dan Snyder, *University of Miami Hospital Data Incident: July 2012: Letter*, UNIVERSITY OF MIAMI HOSPITAL, http://www.umhdataincident.med.miami.edu/letter.html (last visited Dec. 6, 2012).

[15] *Id.* Claiming to review practices may be solely procedural since the hospital had suffered a breach less than a year prior to this affecting 1,219 patients. Erin McCann, *Miami hospital data breach due to employee offense*, HEALTHCARE IT NEWS (Sept. 11, 2012), http://www.healthcareitnews.com/news/u-miami-data-breach-due-employee-offense.

disconcerting that breaches can come from outside the organization and remain unknown until there is harm. In August 2012, it was disclosed to the media that hackers had encrypted a server of The Surgeons of Lake County which stored electronic medical records.[16] They demanded payment in return for the password, oblivious to the fact that the doctors were capable of turning off the server and rendering it inaccessible to either party.[17] Both cases demonstrate the increasing dangers to the privacy and security of patients as more health records are converted to electronic records.

B. The Accretive Health Breach

In 2011, two laptops were stolen from employees of Accretive Health Inc. in Minnesota, resulting in the disclosure of over 23,000 personal health records.[18] The data contained on the laptops was unencrypted and disclosed information such as the patient's name, address, phone number, date of birth, Social Security Number, and diagnostic information.[19] Accretive Health did utilize an encryption system, but the system was not up to date on 30 of the 1,400 laptops in use and these two particular laptops, while being password protected, were not encryption compliant.[20] What distinguishes this case from the Miami University case is that Accretive is not a HIPAA covered-entity; it was a business associate of two Minnesota hospitals: Fairview Health Services and North Memorial Health Care.[21]

---

[16] Jordan Robertson, *Hackers Encrypt Health Records and Hold Data for Ransom*, BLOOMBERG (Aug. 10, 2012, 1:00 PM), http://www.bloomberg.com/news/2012-08-10/hackers-encrypt-health-records-and-hold-data-for-ransom.html.
[17] *Id.*
[18] *Response to Inquiry by Senator Al Franken*, ACCRETIVE HEALTH (May 11, 2012), http://docs.ismgcorp.com/files/external/2012_05_11_Franken_Response.pdf [hereinafter *Franken Response*]. *See also* Second Amended and Supplemental Complaint at 20-26, State v. Accretive Health, Inc., No. 12-145 RHK/JJK (D. Minn. 2012), 2012 WL 2891151 [hereinafter Accretive Complaint].
[19] *Franken Response supra* note 18.
[20] *Id.*
[21] Accretive Complaint *supra* note 18 at 1, 13.

Accretive Health manages the "Revenue Cycle Operations" of client hospitals.[22] Their functions include "scheduling, eligibility verification, registration, admissions, coding and clinical documentation, dealing with third party payors, billing, and collection and payment functions."[23] The HITECH amendments to HIPAA included business associates under the Breach Notification Rule and, as such, they must meet many of the same standards as covered entities.[24] Accretive failed to live up to many of these standards and were alleged to have failed to limit access to patient data only to those employees that needed access, failed to use a limited data set, failed to meet minimum encryption requirements, and failed to sufficiently train employees.[25] Under the statutory cause of action, Minnesota State Attorney General, Lori Swanson, brought a civil action on behalf of the affected clients.[26]

The parties settled, agreeing to monetary damages of $2,490,400 to be paid to the patients, the administration of the settlement, and remaining funds to the Treasury of the State.[27] This amounted to $100 per affected patient, the maximum amount permitted, but exceeded the statutory limitation of $25,000 in a single calendar year.[28] The settlement also enjoined Accretive from operating within the state for a period of six years, a remedy that is unprecedented in HITECH Breach Notification Rule case law.[29] While this may seem like a substantial penalty, Accretive shareholders anticipated much worse and the stock price rose 37%

[22] Accretive Complaint *supra* note 18 at 24.
[23] Accretive Complaint *supra* note 18 at 24.
[24] 42 U.S.C.A. § 17932.
[25] Accretive Complaint *supra* note 18 at 47, 49, 58.
[26] 42 U.S.C.A. § 1320d-5(d); *See generally* Accretive Complaint *supra* note 18. The action included count against Accretive for the use of unlawful collections practices.
[27] Settlement Agreement, Release and Order at 17, State v. Accretive Health, Inc., No. 12-145 RHK/JJK (D. Minn. 2012) , 2012 WL 3065397 [hereinafter Accretive Settlement].
[28] 42 U.S.C.A. § 1320d-5(d)(2).
[29] Accretive Settlement *supra* note 27 at 13-16.

the day the settlement was announced.[30] The fine is relatively insubstantial given Accretive is valued at around $1.2 billion and had a net income of over $29 million in 2011.[31]

The Accretive case is best illustrative of the insufficient penalties to breaching parties. The Department of Health and Human Services may first bring an action under the Breach Notification Rule, but the monetary penalties are not to exceed $1.5 million during a calendar year.[32] Had the Accretive case been brought to trial and ruled for the State, monetary damages for the breach would have been limited to $25,000, so the settlement penalty was focused more on improper collections practices rather than the breach of patient data.[33] With such inadequate penalties and the inexistence of a finalized rule, HHS cannot expect covered entities and business associates to invest in the required safeguards that would protect personal health records from breach.

II. THE STATUTORY TEXT OF THE BREACH NOTIFICATION RULE UNDER HITECH

While this paper also examines safeguards to data breach and proposed amendments to the damages applicable under HIPAA, it is necessary to detail the statutory text of the Breach Notification Rule as guidance for the covered entities and business associates governed by the rule. Covered entities include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form.[34] The term business associate encompasses those whom perform or assist in the performance of a function or activity involving the *use or disclosure* of individually identifiable health information.[35] In this context,

[30] Brian D. Pacampara, *Why Accretive Health Shares Skyrocketed*, THE MOTLEY FOOL (July 31, 2012), http://www.fool.com/investing/general/2012/07/31/why-accretive-health-shares-skyrocketed.aspx?source=itxsitmot0000001&lidx=6.
[31] *Accretive Health, Inc. (AH)*, YAHOO! FINANCE, http://finance.yahoo.com/q?s=AH, (last visited Oct. 17, 2012).
[32] 42 U.S.C.A. § 1320d-5(a)(3)(D).
[33] 42 U.S.C.A. § 1320d-5(d)(2).
[34] 45 C.F.R. § 160.102.
[35] 45 C.F.R. § 160.103 (emphasis added).

"disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information."[36] Under the rule:

> A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information…in the case of a breach…[must] notify each individual whose unsecured protected health information has been or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosure as a result of such breach.[37]

The Code of Federal Regulations defines a breach as "the acquisition, access, use, or disclosure of protected heath information…which compromises the security or privacy of the protected health information."[38] It is important to note that this includes actions like improper disposal of health records, where the data is not actually used or seen by a third party.

Once a breach occurs, there are a number of requirements that the covered entity or business associate must comply with. First, notifications must be made without unreasonable delay and in no later than 60 days after the discovery of the breach.[39] Notification must be made to all affected individuals by first class mail and should be posted on the homepage of the entity's web site if there are 10 or more individuals with insufficient contact information.[40] If the breach affects 500 or more individuals within a state or jurisdiction, then notification must be made to prominent media outlets within the state; and notification must be made to the Secretary of the Department of Health and Human Services regardless of the size of the breach.[41]

The notifications must include a description of the breach, a description of the unsecured health information that was breached, how individuals should protect themselves from potential

[36] 45 C.F.R. § 160.103.
[37] 42 U.S.C. § 17932.
[38] 45 C.F.R. §164.402.
[39] 42 U.S.C. § 17932(d). There is provision delaying notification if requested by law enforcement.
[40] 42 U.S.C. § 17932(e).
[41] 42 U.S.C. § 17932(e). Notification to the Secretary need not be immediate breaches affecting less than 500.

harm, a description of how the entity will investigate the breach, mitigate losses, and protect from future breaches, and contact information for individuals to contact the entity.[42]

III. THE VALUE OF HEALTH INFORMATION: HOW AND WHY THE DATA IS BREACHED

There are several factors that explain why the number of health data breaches has been remarkably high since the HITECH Act was passed in 2009. The most apparent reasons include the shift of medical records to electronic form, the resistance shown by doctors and hospitals in converting their records, and the natural time it takes for federal regulations to be issued and for entities to come under compliance with those regulations.

Initially, the push towards electronic health records was an objective of the George W. Bush administration.[43] At the time less than 10 percent of physicians were using electronic records.[44] The HITECH Act was passed in 2009 and included a "meaningful use" provision which gives government-backed incentives to doctors and eligible hospitals for converting their paper records and filing systems to electronic health records, among several other technology based objectives.[45] In 2011, only 55 percent of physicians had taken the leap with resistance from older physicians and smaller practices.[46] This shift to digitalization means that patients are becoming increasingly susceptible to medical data breach because it is now more accessible and more valuable.

A. Causes of Health Data Breach

---

[42] 42 U.S.C. § 17932(f).
[43] Alvin Powell, *U.S. Lagging in adoption of electronic health records*, HARVARD UNIVERSITY GAZETTE (Oct. 12, 2006), http://www.news.harvard.edu/gazette/2006/10.12/13-healthrecords.html; *see also* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. Ill. L. Rev. 681, 681(2007).
[44] *Id.*
[45] *See generally* Nicholas P. Terry, *Certification and Meaningful Use: Reframing Adoption of Electronic Health Records as a Qualitative Imperative*, 8 Ind. Health L. Rev. 43 (2011).
[46] Jamoom, Eric et al, *Physician Adoption of Electronic Health Record Systems: United States, 2011*, NCHS Data Brief 98 (July 2012), http://www.cdc.gov/nchs/data/databriefs/db98.pdf.

As of November 2012, there have been over 500 reported cases of health data breaches affecting 500 or more and these breaches have affected over 21 million patients.[47] Theft is now the most prevalent form of breach affecting covered entities and business associates, constituting over half of the breaches affecting 500 or more.[48] This is logical since stealing thousands of electronic health records is far easier than stealing a filing cabinet full of patient folders, although nearly a quarter of these breaches involved paper records.[49]

Paper records are far more susceptible to improper disposal, loss, and improper access, while electronic records stored on laptops, desktop computers, or portable electronic devices are generally the cause of breaches by theft.[50] This harps on both the accessibility and the value of health data that is stored electronically. The records are more accessible because more people have access to them, especially when the records are interoperable and accessed through networked hard drives. For instance, stolen laptops, which can either house the data or access it, have been one of the major causes of data breaches and this generally results from simple carelessness.[51]

The fact that it is likely that there will be more records in a concentrated place makes the records more valuable to identity thieves. Identify theft can come in the form of either financial

[47] *BAs Involved in One of Nine New Reported Breaches*, HIPAA & BREACH ENFORCEMENT STATISTICS FOR DECEMBER 2012, http://www.melamedia.com/HIPAA.Stats.home.html (last visited Dec. 6, 2012).
[48] Keckley, Paul H. et al, *Privacy and Security in Health Care: A fresh look*, DELOITTE, available at http://www.deloitte.com/us/privacyandsecurityinhealthcare#. [hereinafter Deloitte]. *See also* David Holtzman, Breach Notification for HIPAA Covered Entities and Business Associates at the NIST/OCR HIPAA Security Conference (June 7, 2012) *available at* http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-4_dholtzman_ocr-hitech-breach-notifcation-rule.pdf [hereinafter Holtzman Presentation].
[49] Holtzman Presentation *supra* note 48.
[50] *Breaches Affecting 500 or More Individuals*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Dec. 6, 2012).
[51] Deloitte *supra* note 48 at 2.

identity theft or medical theft, the dangers of which are both well documented.[52] One's medical identity can be used by others to receive medical treatment, potentially at the cost of the aggrieved party.[53] While it is often the case that a stolen laptop will not result in identity theft because the purpose of theft was the hardware and not it's content, there are a number of cases of data being stolen for the purpose of identity theft and this is why compliance with the Privacy and Security Rules is so imperative.

B. Consequential Costs of a Health Data Breach to a Covered Entity

It is no secret that health data breaches can be extremely costly to the covered entity. A 2011 study on the costs of data breaches found that the cost per record lost in the healthcare industry was $240, making healthcare the fourth most costly among the industries examined.[54] Another study found that the average medical data breach resulted in over $2 million in related expenses.[55] These costs did not include monetary penalties sanctioned by the government, which could reach as high as $1.5 million, or resulting lawsuits brought by the patients.[56]

The consequential costs of a breach would include actions the covered entity must take in reacting to the breach such as: investigating the breach, mailing notices to patients, offering credit monitoring services to the patients, and hiring counsel.[57] On top of these costs there are others that are not as easily calculated, like time and productivity loss, brand or reputation loss,

[52] *Second Annual Benchmark Study on Patient Privacy & Data Security*, PONEMON INSTITUTE at 16 (Dec. 2011), http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf. [hereinafter Ponemon Study].
[53] *Medical Identity Theft*, WWW.IDENTITYTHEFT.INFO, http://www.identitytheft.info/medical.aspx (last visited Dec. 6, 2012).
[54] *2011 Cost of Data Breach Study*, PONEMON INSTITUTE at 15 (Mar. 2012), http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US.
[55] Ponemon Study, *supra* note 52 at 1.
[56] The statutory authority on monetary fines is discussed *infra*, as is an analysis of pending class action suits brought under state privacy laws.
[57] Ponemon Study, *supra* note 52 at 1.

and loss of patient goodwill.[58] At 4.2%, the healthcare industry has one of the highest "churn" rates, the percentage of patients who will no longer use the provider after a breach of personal information.[59] Each of these patients is worth over $100,000 over the course of their lifetime, so a hypothetical breach affecting 1,000 patients could cost the entity $4.2 million in loss of patient goodwill alone.[60] Taking this into account, in addition to the monetary fines, civil liability, and other related costs, a covered entity would likely lose several million dollars in dealing with a data breach. Unfortunately, these costs, offset by the risk of suffering from a data breach, often do not constitute enough of an expense to encourage covered entities to improve their existing data security protocol.[61]

IV. Steps Covered Entities and Business Associates Should Take to Comply and Safeguard Electronic Health Data

As the use of electronic health records has risen, so too has the use of information technology consultants and internal HIPAA compliance officers.[62] However, despite the availability of hundreds of information technology security firms, there are many basic steps that covered entities and business associates could take to meet statutory requirements, best deter the chance of data breach, and to alleviate the costs and damages post breach.

A. Federal Regulations

The first step in properly protecting patient data is by meeting the baseline federal requirements on personal health information privacy. The Department of Health and Human Services has the statutory authority to issue regulations and guidance on the interim Breach

[58] Ponemon Study, *supra* note 52 at 1.
[59] *2011 Cost of Data Breach Study*, Ponemon Institute at 7 (Mar. 2012), http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US.
[60] Ponemon Study, *supra* note 52 at 2.
[61] *Id.* at 2.
[62] Bernie Monegain, *High demand for Health IT consulting*, Healthcare IT News (Oct. 2, 2012), http://www.healthcareitnews.com/news/high-demand-health-it-consulting.

Notification Rule under HITECH and under the HIPAA Privacy and Security Rules.[63] The importance of complying with these regulations cannot be understated. The general enforcement of these rules has been scarce, but upon a data breach of 500 or more the Office of Civil Rights will perform a review assessing the cause of the breach, compliance with the Privacy and Security Rules, and how the breach has been handled.[64] HHS has discretion in issuing a monetary penalty based on the OCR report and is far more likely to do so when there is a lack of compliance because these constitute additional violations.[65]

The regulations state that some rules are requirements, while others are merely addressable issues and their utilization should take into account factors such as the size of the covered entity, its technical infrastructure, the costs of the security measurements, and the probability of potential risks.[66] Complying with these considerations should not call for a drastic overhaul of a covered entity's existing protocol and exist to set minimum requirements that entities should hope to exceed. Unfortunately, many covered entities fail to meet even these standards.[67]

In 2011, the Office of Inspector General released the results of an audit of seven covered entities conducted between October 2008 and March 2010 and concluded that the Centers for Medicare & Medicaid Services were not sufficiently ensuring compliance by covered entities of the HIPAA Security Rule.[68] The investigation uncovered 151 specific vulnerabilities (124 of which were deemed high impact) in the protection of electronic personal health information

[63] 42 U.S.C. § 17932(j); 42 U.S.C. § 1320d-2(264).
[64] Holtzman Presentation *supra* note 48.
[65] *See generally Your Health and Your Privacy: Protecting Heath Information in a Digital World: Hearing Before the Subcomm. On Privacy, Technology, and the Law*, 112th Cong. (2011), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=9b6937d5e931a0b792d258d9b332c04d.
[66] 45 C.F.R. § 164.306(b).
[67] Daniel R. Levinson, *Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight*, Office of Inspector General, May 2011 [hereinafter OIG Report].
[68] *Id.* at iii.

(ePHI) that left the covered entities susceptible to data breach.[69] These vulnerabilities are helpful in examining the following federal regulations which are divided into administrative safeguards, physical safeguards, and technical safeguards.

1. Administrative Safeguards

The Administrative Safeguards listed within the Federal Regulations outline a number of general concerns that the corporate policies and procedures of covered entities should seek to comply with. Specifically, rules should be in place in determining who may access and work with certain ePHI and who may enter the areas in which the information is stored.[70] Additionally, procedures should be developed to quickly verify whether ePHI has been accessed by an authorized or unauthorized workforce member, along with procedures for terminating access to the material when an employee is dismissed or leaves the position.[71]

In order to properly implement these procedures it is essential that the entity's security software is consistently updated to account for evolving threats and malicious software.[72] The system should be sophisticated enough to produce audit trails for personal log-in attempts with automatic alerts for discrepancies.[73] In this regard, the software should allow for the creation of user passwords, which need to be changed periodically.[74] The passwords should be properly safeguarded in terms of data protection and in terms of employee disregard for their purpose.[75]

The entity must create a contingency plan in case of emergencies, such as fire, vandalism, system failure, or natural disaster.[76] The plan must call for the maintenance of backup exact

[69] *Id.*
[70] 45 C.F.R. § 164.308(a)(3).
[71] *Id.*
[72] 45 C.F.R. § 164.308(a)(5).
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] 45 C.F.R. § 164.308(a)(7).

copies of ePHI and a means of recovering any lost data.[77] The entity must also create a protocol for emergency mode operation, meaning they must be able to continue to perform critical business processes while dealing with the emergency.[78]

2. Physical Safeguards

The Federal Regulations define physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusions."[79] The safeguards are mainly designed as a means of enforcing the administrative safeguards noted above. For example, the administrative safeguards require entities to have policies as to whom may have access to areas where ePHI is stored and the physical safeguards require policies that limit physical access to these areas.[80] This includes not only where the data is stored, but also restriction of physical access to workstations that may contain ePHI.[81]

Another physical safeguard that entities must comply with is proper disposal of ePHI.[82] This requires the implementation of policies and procedures to remove and dispose of records from electronic media before it's re-use.[83] The regulations also recommend that entities maintain records of hardware and electronic media and those responsible for handling it and that entities create exact copies of ePHI before physical movement of the equipment.[84]

---

[77] *Id.*
[78] *Id.*
[79] 45 C.F.R. § 164.304.
[80] 45 C.F.R. § 164.310(a)(1).
[81] *Id.*
[82] 45 C.F.R. § 164.310(d)(2).
[83] *Id.*
[84] *Id.*

The dangers of failing to ensure proper destruction of ePHI was experienced by the Brighton and Sussex University Hospitals NHS Trust in April of 2010 in the United Kingdom.[85] The hospital had employed a contractor, Sussex Health Informatics Service, to destroy approximately 1,000 hard drives that were no longer in use.[86] An employee of Sussex Health, who had access to the key code protected room holding the hard drives, removed at least 252 of the hard drives and sold at least 232 online.[87] The hard drives, which had been used in the HIV and Genito Urinary Medicine Department, contained extremely personal data including: "names; date of birth; occupations; sexual preferences; STD test results and diagnoses for 67,642 patients in readable format."[88] This resulted in a monetary fine of £325,000 from the Information Commission's Office under the Data Protection Act, taking account for the seriousness and highly sensitive nature of the data.[89]

A similar situation occurred stateside in 2009, when unencrypted hard drives were stolen from a closed call-center facility.[90] In that case, the call-center was leased by BlueCross BlueShield of Tennessee and the facility was not properly safeguarded upon closure.[91] 57 hard drives were stolen containing "member names, Social Security numbers, diagnoses codes, dates of birth and health plan identification numbers" and resulted in a $1.5 million fine.[92]

---

[85] *NHS Trust fined £325,000 following data breach affecting thousands of patients and staff*, INFORMATION COMMISSIONER'S OFFICE (June 1, 2012), http://www.ico.gov.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012.aspx.
[86] Jeffrey Roman, *Largest UK Breach Penalty Appealed*, DATA BREACH TODAY (June 4, 2012), http://www.databreachtoday.asia/largest-uk-breach-penalty-appealed-a-4823.
[87] *Id.*
[88] Press Release, Information Commission's Office, Data Protection Act 1998: Monetary Penalty Notice at 3 (May 28, 2012), *available at* http://www.ico.gov.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012.aspx.
[89] *Id.* at 8, 10.
[90] Howard Anderson, *BCBS of Tenn. Gets $1.5 Million Penalty*, HEALTHCARE INFO SECURITY (Mar. 13, 2012), http://www.healthcareinfosecurity.com/bcbs-tenn-gets-15-million-penalty-a-4583.
[91] *Id.*
[92] *Id.*

These cases illustrate some of the precautions entities should take in destroying ePHI and cleaning the electronic media on which it was stored. Under HITECH, the third party responsible for removing and destroying the data in the Brighton and Sussex case would be governed as business associate. Covered entities would want to ensure that there is a contract between the entity and the third party, expressly designating the third party as a business associate.[93] As per the BlueCross BlueShield of Tennessee case, arrangements should have been made to destroy the data at the beginning of the foreclosure proceedings.

The Department of Health and Human Services has specified the means to which health information should be destroyed.[94] If the data is in the form of paper, film, or other hard copy media it must be "shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed."[95] Electronic media must be "cleared, purged, or destroyed" so that it cannot be retrieved and meet the National Institute of Standards and Technology (NIST) requirements for Media Sanitation.[96] Like the other Federal Regulations, these are small steps that the entities should have accounted for in order to avoid breach and the resulting penalties.

3. Technical Safeguards

The technical safeguards of the Code of Federal Regulations address specific concerns about the operability of software.[97] First, the software must assign unique identifiers to each user and track usage.[98] The software must also allow for emergency access to the data as necessary.[99]

---

[93] 45 C.F.R. § 164.308(b)(1); see also 45 C.F.R. § 164.314.
[94] 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, 74 Fed. Reg. 19006 (Apr. 27, 2009) (45 CFR Parts 160 and 164) [hereinafter HHS Unusable Guidance].
[95] *Id.*
[96] *Id.* NIST Guidelines for Media Sanitation *available at* http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf.
[97] 45 C.F.R. § 164.312.
[98] 45 C.F.R. § 164.312(a)(2).

The Regulations recommend that the software have an automatic log-off function to terminate access after a predetermined period of time, that unauthorized alterations to ePHI be detected, and that the software use encryption and decryption techniques.[100]

Like the guidance on destruction of data, HHS has also issued guidance on data encryption.[101] Meeting this standard is incredibly important because if the data is properly encrypted, it is rendered "unusable, unreadable, or indecipherable to unauthorized individuals" and is therefore not subject to the Breach Notification Rule.[102] The Regulations define encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[103] To meet the HIPAA standard the confidential process or key that enables decryption must not have been breached.[104] The encryption methods must meet NIST standards for data at rest and Federal Information Processing Standards (FIPS) for data in motion.[105]

B. Other Compliance Measures to Reduce Data Breaches

There are a number of other ways for a covered entity to safeguard itself from breaches of health data. Some are more expensive than simply complying with the Federal Regulations above, but if properly implemented they could save a great deal of money in avoiding breach. Additionally, by taking these steps a covered entity would reduce the chance that HHS would levy fines against it in the event of a breach.

First, the covered entity should choose HIPAA compliant software when converting to or updating EHR. This should meet minimum encryption and password standards. Next, covered

---

[99] *Id.*
[100] *Id.*
[101] HHS Unusable Guidance, *supra* note 94.
[102] *Id.*
[103] 45 C.F.R. § 164.304.
[104] HHS Unusable Guidance, supra note 94.
[105] *Id.* The NIST standard is available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf and the FIPS standard is available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

entities should limit the access to data via portable devices and keep data stored on central hard drives accessed over the cloud. To help contrive and monitor the protocol, the covered entity should hire a compliance/security officer. This officer should then give regular training to employees about the Privacy and Security Rules, as well as developing incident response plans and performing risk assessments.

V. THE INADEQUACY OF THE CURRENT CIVIL MONETARY PENALTIES

The number of data breaches that have occurred since the passage of HITECH is terribly alarming and tends to support the notion that the current regulation of personal health information is inadequate in deterring future breaches, especially when the breaches are caused by such preventable and identifiable causes. The most apparent issue is that the current monetary penalties are not significant enough to encourage a breaching entity to alter their standards and procedures and they are by no means strong enough to encourage other entities to do likewise. The resistance of covered entities is also the result of a lack enforcement of the Privacy and Security Rules. The probability of facing a monetary penalty following a breach is low so the potential costs to the entity are reduced by this likeliness.

The current statutory framework of the Breach Notification Rule grants two separate causes of action to address health data breaches: one to the Secretary of the Department of Health and Human Services and one to the attorney general of the state in which the breach occurred.[106] However, currently there is no federal private cause of action for aggrieved patients.

A. Actions Brought by the Department of Health and Human Services

The penalties HHS may impose vary by degree of culpability (reasonable cause, willful neglect, unknowing) but all may reach a maximum of $50,000 for each violation, not to exceed

[106] 42 U.S.C. § 1320d-5.

$1,500,000 for a single violation that occurs within a calendar year.[107] Generally, these suits are not brought before a court and are settled between the parties.[108] This allows for the parties to work together amicably in developing a resolution and avoid the time and money of going to court.

1. Corrective Action Plans

The resolutions typically result in a Corrective Action Plan (CAP) that the entity must abide by by meeting specified security standards and issuing regular reports to the Office of Civil Rights. A good example of the process involved the Massachusetts Eye and Ear Infirmary (MEEI), who settled with HHS in September 2012.[109] Two years early, a neurologist of MEEI was traveling in South Korea and was the victim of a stolen laptop containing unencrypted information on over 3,500 patients.[110] The doctor notified HHS and subsequently, OCR began its investigation of the breach and of the hospital's security practices.[111] Upon the investigation, OCR concluded that the hospital had failed to meet several elements of the Security Rule, Privacy Rule, and Breach Notification Rule.[112] In reaching a Resolution Agreement, the parties agreed that $1,500,000 would be paid over three years and a Corrective Action Plan was developed to remedy the malfeasances and ensure future compliance.[113]

---

[107] 42 U.S.C. § 1320d-5(a).
[108] *See Case Examples and Resolution Agreements*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Dec. 6, 2012).
[109] *Massachusetts provider settles HIPAA case for $1.5 million*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html (last visited Dec. 6, 2012).
[110] Marianna Kolbasuk McGee, *Another Big Fine After a Small Breach*, DATA BREACH TODAY (Sept. 17, 2012), http://www.databreachtoday.com/another-big-fine-after-small-breach-a-5116.
[111] Press Release, Department of Health & Human Services, Massachusetts provider settles HIPAA case for $1.5 million (Sept. 17, 2012), *available at* http://www.hhs.gov/news/press/2012pres/09/20120917a.html.
[112] *Id.*
[113] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights, and the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (last visited Dec. 6, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf.

The Resolution Agreement specified six areas of conduct that were in violation of HHS regulations.[114] These areas were: (1) failure to perform an on-going risk analysis, (2) insufficient security measures to secure confidentially of ePHI, (3) lack of an incident response plan, (4) lack of policies restricting use of portable devices only to those authorized, (5) lack of policies tracking receipt and removal of portable devices, and (6) failure to encrypt data.[115] These issues were taken into consideration in creating a three-year CAP requiring Annual Reports and document retention.[116]

First, the CAP requires that MEEI develop policies and procedures to meet the Federal standards and submit the plan to HHS for approval.[117] Second, the approved plan must be distributed to all members of MEEI's workforce that have access to ePHI, who must then sign a compliance certificate before re-accessing ePHI.[118] Next, MEEI must create additional procedures to investigate matters involving workforce members who fail to comply with the policies and procedures, along with providing required training.[119] Lastly, MEEI must designate an independent compliance officer with expertise in compliance of the Security Rule to monitor the implementation of the plan, including performing unannounced audits, reviewing document retention, and preparing reports to HHS, among other duties.[120] The Implementation Report and Annual Reports required to be submitted to HHS must include various certifications regarding the policies that have been implemented, copies of training materials, monitor findings, and a summary of any Reportable Events.[121]

---

[114] *Id.* at 1-2.
[115] *Id.*
[116] *Id.* at A-2.
[117] *Id.* at A-3. The CAP includes a list of 10 factors that the plan must include into to gain approval. *Id* at A-4.
[118] *Id.*
[119] *Id.* at A-5.
[120] *Id.* at A-5-A-7.
[121] *Id.* at A-8-A-9.

The MEEI settlement is fairly representative of the enforcement taken by HHS upon a data breach by a covered entity or business associate. The Resolution Agreement allows HHS and the entity to develop a CAP that is particularized to the concerns of the entity. However, the requirements of the CAP are essentially nothing more than mandatory reporting. The plan that MEEI was required to implement is a culmination of provisions listed within the Federal Regulations, meaning they are rules that MEEI should already have been complying with.

2. Lack of deterrence

Another point that the MEEI case illustrates is that the CAP and monetary penalty do not sufficiently act as deterrence against future breaches. The breach discussed above was MEEI's second data breach in less than six months.[122] The first breach occurred in November 2009 when it was discovered that two employees were misappropriating patient credit cards.[123] The case was reported to HHS under the Breach Notification Rule and no further action was taken against MEEI.[124] After MEEI's second breach, but before the Resolution Agreement with HHS was reached, MEEI suffered from a third breach of patient data.[125] This breach, announced in April 2012, also resulted from employee misconduct.[126] In this instance the employee used patient names, Social Security Numbers, and dates of birth, possibly affecting as many as 3,600 patients.[127] MEEI subsequently gave one year of credit monitoring service to the patients, but

[122] *Breaches Affecting 500 or More Individuals*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Dec. 6, 2012).
[123] Mary Leach, *Mass. Eye and Ear Alerts Patients to Data Breach*, MASSACHUSETTS EYE AND EAR (Jan. 4, 2010), http://www.masseyeandear.org/news/press_releases/recent/important_alert/data-breach/.
[124] *Id. See also* Michael Kline, *As the Breach Parade Passes 500 Marchers; Should There be a Posting on the HSS List for a Third Massachusetts Eye and Ear Infirmary Breach?*, HIPAA, HITECH & HIT (Oct. 28, 2012), http://hipaahealthlaw.foxrothschild.com/2012/10/articles/breaches/as-the-breach-parade-passes-500-marchers-should-there-be-a-posting-on-the-hhs-list-for-a-third-massachusetts-eye-and-ear-infirmary-breach/.
[125] Mary Leach, *Mass. Eye and Ear Alerts Patients to Data Breach*, MASSACHUSETTS EYE AND EAR (Apr. 16, 2012), http://www.masseyeandear.org/news/press_releases/recent/data_breach_2012/.
[126] *Id.*
[127] *Id.*

there was no action brought by HHS and the breach was not addressed in the Resolution Agreement released in September 2012.[128]

This series of data breaches by a single entity emphasizes the lack of a deterrence function in the powers currently held by HHS. Only one of MEEI's three breaches was acted upon and each breach resulted from MEEI's failure to meet HIPAA security regulations. In applying this to other breaches, the odds of having a fine assessed against the covered entity is far less than one in three. Since HITECH was passed only a handful of covered entities or business associates have been assessed a civil monetary penalty by HHS, while the number of breaches requiring patient notice has climbed to over 500.[129] HHS has worked with the entities to correct their noncompliance with the Privacy and Security Rules and has developed CAPs in the absence of a fine.[130]

Even so, the fines levied against the entity are generally insubstantial given the size of the entity and are unlikely to encourage other covered entities to adopt technical and procedural security measures.[131] Under the current law, covered entities are likely to wait for a breach to occur and deal with the resulting investigation than to spend on measures that would prevent the breach.

B. Actions Brought by State Attorney Generals

As noted above, the statutory framework also gives a cause of action to state attorney generals acting as *parens patriae* for the residents of the state.[132] The attorney general can seek damages of $100 per each adversely affected patient, but the total may not exceed $25,000 in a

[128] *Id.*
[129] *See Case Examples and Resolution Agreements*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Dec. 6, 2012).
[130] *Id.*
[131] Marianna Kolbasuk McGee, *Another Big Fine After a Small Breach*, DATA BREACH TODAY (Sept. 17, 2012), http://www.databreachtoday.com/another-big-fine-after-small-breach-a-5116.
[132] 42 U.S.C. § 1320d-5(d).

single calendar year.[133] Like HHS enforcement, this cause of action generally results in settlement rather than trial.[134] Consequently, the attorney generals have more power than it would appear under the statute. As discussed *supra*, the Accretive settlement resulted from several violations in addition to data breach, including state law collections practices and the entity was barred from conducting business in Minnesota for a period of six years and fined $2.5 million.

The first settlement reached under the HITECH Act also resulted in a fine over the statutory limit.[135] The resolution was reached after a breach via a lost computer drive, affecting more than 500,000 Connecticut citizens. The settlement of $250,000 included state law privacy protection violations, in addition to the HIPAA violations, and therefore could exceed the statutory damages cap.[136] A Corrective Action Plan was also required by the settlement, which is not an expressly written remedy under HIPAA.[137] As evidenced by these examples, the monetary penalties levied by state attorney generals, even when exceeding the statutory cap, is incapable of deterring future breaches by the breaching entity or other covered entities.

There are several reasons that may explain why the current level of enforcement by HHS and state attorney generals has not kept pace with the number of significant health data breaches that have occurred since the passage of HITECH. First, HHS may have allowed for leniency in penalizing breaching entities given the novelty of the amendment. HHS has discretion when deciding whether to issue a fine and may take into consideration the size of the breach, the

---

[133] 42 U.S.C. § 1320d-5(d)(2).
[134] *See* Paula Cotter, *Amendments to Health Privacy Law Grants States Enforcement Powers*, NATION ASSOCIATION OF ATTORNEYS GENERAL GAZETTE, http://www.naag.org/amendments-to-health-privacy-law-grant-states-enforcement-powers.php (last visited Dec. 6, 2012).
[135] *Health Net Settles With Connecticut Over Massive Security Breach*, CTWATCHDOG.COM (July 6, 2010) http://ctwatchdog.com/health/health-net-settles-with-connecticut-over-massive-security-breach.
[136] Press Release, State of Connecticut Office of the Attorney General, Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info (July 6, 2010) (available at http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754).
[137] *Id.*

amount of harm resulting from the breach, and how the entity responded to the breach. Additionally, the Breach Notification Rule, and parts of the Privacy and Security Rules, have not been finalized so it may be unreasonable to expect covered entities to spend on security when the measures they adopt may not be in compliance once a final rule is adopted.

Second, there may have been an internal decision that the limited resources of HHS and OCR are better allocated battling other areas of concern. For instance, HHS has recently implemented an overhauled auditing system to detect fraud in the Medicare and Medicaid context.[138] There are many instances of breach where there is no resulting harm to the patients and no intentional wrongdoing by the covered entity, so it would be reasonable for HHS to be focusing its efforts on instances of intentional fraud.

Lastly, state attorney generals may be ill-equipped to prosecute health data breach claims. An extensive, two-day training session was offered by HHS to interested state attorney generals in 2011, but the sophistication of the material could still have left the attorney generals feeling unprepared to bring a claim.[139] Moreover, given the $25,000 statutory cap on damages, the attorney generals may have decided that federal enforcement of the Breach Notification Rule is more worthwhile, since state prosecutors also feel the effects of having limited resources and expectations from the public to prosecute egregious crimes.

VI. THE SUCCESS OF PRIVATE CAUSES OF ACTION

While there is no federal private cause of action for individuals who have been the victim of a health data breach, there are some state law protections that offer an opportunity for redress.

---

[138] *See generally* Dr. Peter Budetti, Deputy Administrator and Director of the Center for Program Integrity, Centers for Medicare & Medicaid Services, *Saving Taxpayer Dollars By Curbing Waste and Fraud In Medicaid* before *Committee on Homeland Security and Government Affairs Subcommittee on Federal Financial Management, Government Information, Federal Services, and Internat*, 112th Cong. (June 14, 2012) *available at* http://www.hhs.gov/asl/testify/2012/06/t20120614a.html.

[139] *HIPAA Enforcement Training for State Attorneys General*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/sagmoreinfo.html (last visited Dec. 6, 2012).

Unfortunately, patients have had very little success on this endeavor, though a pending class action in the Eleventh Circuit may reverse this. If successful, it could stand as a model upon which a federal private cause of action could be developed because the damages sought are far greater than statutory caps of the Breach Notification Rule.

There are very few states that offer protection specifically for the breach of medical data, without other factors and many states preempt data disclosure statutes when they are governed by a federal body with similar regulations.[140] However, like actions brought by state attorney generals, there may be underlying state law violations that that are actionable. California currently has the most progressive medical breach statutes, which will be slightly restricted in 2013.[141] This statute and other pending lawsuits are addressed below.

A. California Confidentiality of Medical Information Act

California's Confidentiality of Medical Information Act (CMIA) governs the wrongful disclosure of personal health information.[142] In this regard it is functionally similar to HIPAA, but the CMIA awards nominal damages of $1,000 to aggrieved plaintiffs without a showing of actual damages, and without a statutory maximum.[143] This had led to a number of suits against health care providers, often for substantial sums of alleged damages.[144] There is a general sense that this cause of action will not exist for much longer.[145] The statute was enacted in 1981, prior to the digitalization of medical records, so data breaches involving a large number of plaintiffs

[140] *State Data Security Breach Notification Laws*, MINTZ LEVIN, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (last visited Dec. 6, 2012). Site updated as of September 1, 2012.
[141] Confidentiality of Medical Information Act, Cal. Civ. Code § 56 (West 2012).
[142] *Id.*
[143] Cal. Civ. Code § 56.36(1) (West 2012).
[144] Dan Verel, *Medial data breaches spur lawsuits*, NORTH BAY BUSINESS JOURNAL (Oct. 29, 2012, 6:15 AM), http://www.northbaybusinessjournal.com/63733/medical-data-breaches-spur-lawsuits/.
[145] Taylor Armerding, *Law firms see big money in healthcare breach cases*, CSO SECURITY AND RISK (Apr. 16, 2012), http://www.csoonline.com/article/704288/law-firms-see-big-money-in-healthcare-breach-cases.

were unprecedented.[146] Additionally, prior to breach notification laws patients would not have known about an improper disclosure of their health record unless they suffered a resulting harm. Now that plaintiffs must be notified, claims based on harmless data breaches have been filed and courts have been resistant to certify a class absent actual harm.

As of this writing, no cases have awarded damages for breach, but again, several class actions have been commenced, including one against IBM—as a business associate of Health Net—that is worth over a billion dollars under the statute.[147] The Health Net case was removed to a Federal District Court and later dismissed for lack of standing insofar as the plaintiffs were asserting conjectured harm.[148] The downfall of the plaintiffs was likely the removal to a federal court which applied a federal standing standard.

Another breach occurred in September 2011 at the UCLA Health System.[149] A hard drive was stolen from a physician's home with information on 16,000 patients and a class action was filed in the Superior Court of Los Angeles in December 2011.[150] On October 30, 2012, the plaintiff's complaint was filed with the court with the CMIA being the only cause of action and seeking the award of nominal damages for all parties to be named in the case.[151] This has the potential to result in damages of over $16 million, a substantial amount greater than the $1.5 million permitted under HIPAA.[152]

---

[146] *Id.*
[147] *Health Net & IBM Data Breach Class Action Lawsuit*, GIRARD GIBBS LLP, HTTP://WWW.GIRARDGIBBS.COM/CASE/25/HEALTH-NET-IBM-PRIVACY-BREACH/ (last visited Dec. 6, 2012).
[148] Whitaker v. Health Net of California, Inc., CIV S-11-0910 KJM-DAD 2012 WL 174961 (E.D. Cal. Jan. 20, 2012).
[149] Daniel Riesenbach, *Class-action lawsuit against UCLA Health System for data breach fails to move forward*, UCLA DAILY BRUIN (Jan. 10, 2012, 4:56 AM), http://www.dailybruin.com/index.php/article/2012/01/classaction_lawsuit_against_ucla_health_system_for_data_breach_fails_to_move_foward.
[150] *Id.*
[151] Class Action Complaint at 9, Platter v. Regents of the Univ. of Cal. at Los Angeles Health Sys. (Cal. Super.) (No. BC494928), 2012 WL 5338750.
[152] *Id.*

This case and others against Sutter Health for $4.25 billion,[153] St. Joseph Health System for $31.8 million,[154] and Stanford Hospital & Clinics for $20 million[155] should sufficiently put health care providers on notice of the need to properly secure their data, even if the damages are not awarded. Again, if these cases proceed they will result in far more damages than under HIPAA and will go towards the patients rather than HHS or the state. This begs the question: which is the better deterrent against personal health information? If an entity's greatest concern in updating their privacy and security measures is cost, then the higher recoveries are surely a better means of encouraging upgrades in systems and policies and meeting the minimums of the federal regulations. However, the size of the awards may be so detrimental to the entities that they would be less willing to shift to using ePHI to begin with.

The California legislature has taken the first steps in addressing the size of the class action suits by amending the current law to add an affirmative defense for the entity to take effect on January 1, 2013.[156] The affirmative defense is very limited in its coverage in that the disclosure of confidential information must have been made to another covered entity or business associate and may not have been an incident of medical theft.[157] In addition, the entity must have been complying with current best practices under HIPAA and properly responded to the breach.[158] Moreover, the entity that received the confidential information must have destroyed

[153] Kathy Robertson, *Hearing scheduled on Sutter data breach class action*, SACRAMENTO BUSINESS JOURNAL (Sept. 21, 2012, 6:33 AM), http://www.bizjournals.com/sacramento/news/2012/09/21/hearing-scheduled-sutter-data-suit.html?page=all.
[154] Taylor Armerding, *Law firms see big money in healthcare breach cases*, CSO SECURITY AND RISK (Apr. 16, 2012), http://www.csoonline.com/article/704288/law-firms-see-big-money-in-healthcare-breach-cases.
[155] *Lawsuit Filed Against Stanford Following Patient Data Breach*, CALIFORNIA HEALTHLINE (Oct. 4, 2011), http://www.californiahealthline.org/articles/2011/10/4/lawsuit-filed-against-stanford-following-patient-data-breach.aspx.
[156] Michael Epshteyn , *California Adds Affirmative Defense to Medical Privacy Law*, CHRONICLE OF DATA PROTECTION (Oct. 4, 2012), http://www.hldataprotection.com/2012/10/articles/health-privacy-hipaa/california-adds-affirmative-defense-to-medical-privacy-law/#more.
[157] 2012 Cal. Legis. Serv. Ch. 437 (A.B. No. 439) (West).
[158] *Id.*

or returned the records and not retained, used, or released them.[159] In effect, this amendment would do little to alter the current state of the pending class actions since several were the result of theft.[160] It may not be until one of these cases is finalized that the legislature decides to act on this, or they feel that this is a good law and support it.

B. Class Actions Under Non-medical State Disclosure Laws

In addition to California's private cause of action for the breach of medical data, private causes of action may exist for the disclosure of personal information in the non-medical context that would allow patients to recover for the breach of their ePHI. Currently, there are pending cases surrounding three incidents of breach that may establish liability to health care providers. Previous cases have met resistance from the courts because the plaintiffs have failed to establish any actual harm.[161] In *Paul v. Providence Health Sys.-Oregon*, the Oregon Supreme Court affirmed the dismissal of a class action suit resulting from the negligent loss of computer disks containing the records of 365,000 patients.[162] The plaintiffs to the suit alleged negligence and sought the cost of credit monitoring services.[163] In dismissing, the Court held that the credit monitoring is a cost against a possible future harm and is not actionable under the state's Unfair Trade Practices Act absent a showing of actual harm.[164]

---

[159] *Id.*
[160] Daniel Riesenbach, *Class-action lawsuit against UCLA Health System for data breach fails to move forward*, UCLA DAILY BRUIN (Jan. 10, 2012, 4:56 AM), http://www.dailybruin.com/index.php/article/2012/01/classaction_lawsuit_against_ucla_health_system_for_data_breach_fails_to_move_foward.
[161] Sang Lee, *Data Security Breach Costs: Emory Healthcare Sued For $200 Million Over 10 CDs*, ALERTBOOT ENDPOINT SECURITY (June 16, 2012, 12:48 AM), http://www.alertboot.com/blog/blogs/endpoint_security/archive/2012/06/16/data-security-breach-costs-emory-healthcare-sued-for-200-million-over-10-cds.aspx.
[162] 351 Or. 587, 589 (2012).
[163] *Id.* at 590.
[164] *Id.* at 603.

A comparable case in a Georgia state court may face a similar fate.[165] In June 2012, a class action complaint was filed against Emory Healthcare Inc. in Fulton County Superior Court alleging violations of Georgia state laws.[166] The case stems from a February 2012 theft of computer disks with the confidential information of over 315,000 patients, including names and Social Security Numbers.[167] The complaint alleges causes of action for invasion of privacy, negligence, negligence *per se*, and breach of implied contract as tortious claims; and seeks nominal damages of $1,000 per class member and three years of credit monitoring, along with actual damages and exemplary damages.[168] Without a statutory right to nominal damages, like the California statute, this class action is likely to fail for remoteness.[169]

A trio of other class action suits have resulted from the theft of computer tapes stolen from the vehicle of an employee of Science Applications International Inc. (SAIC) in September 2011, with the health information of 4.9 million patients.[170] TRICARE is the health care provider of active duty, retired, and family members of military personnel.[171] SAIC is a contractor of TRICARE and has been sued in California state court and a Texas District Court.[172] TRICARE and the United States Department of Defense have been sued in federal court in

---

[165] Sang Lee, *Data Security Breach Costs: Emory Healthcare Sued For $200 Million Over 10 CDs*, ALERTBOOT ENDPOINT SECURITY (June 16, 2012, 12:48 AM), http://www.alertboot.com/blog/blogs/endpoint_security/archive/2012/06/16/data-security-breach-costs-emory-healthcare-sued-for-200-million-over-10-cds.aspx.

[166] Class Action Complaint at 1, Bombardieri v. Emory Healthcare Inc., 2012CV215883 (Ga. Super. 2012), *available at* http://docs.ismgcorp.com/files/external/Emory-Class-Action-Complaint.pdf.

[167] *Id.* at 13-14.

[168] *Id.* at 14-19.

[169] *See* Ga. Code Ann. § 51-12-8 (West 2012) defining remoteness as when the damage incurred is only the imaginary or possible result of a tortious act; such claim is then too remote to be the basis of recovery.

[170] Bob Brewin, *Contractor Hit with Second Class Action Suit Over Tricare Data Theft*, NEXTGOV (Jan. 6, 2012), http://www.nextgov.com/health/2012/01/contractor-hit-with-second-class-action-suit-over-tricare-data-theft/50411/. *See also* Sabrina Rodak, *TRICARE Contractor Faces Second Lawsuit Over September Data Breach*, BECKER'S HOSPITAL REVIEW (Jan. 10, 2012), http://www.beckershospitalreview.com/healthcare-information-technology/tricare-contractor-faces-second-lawsuit-over-september-data-breach.html.

[171] *About TMA*, TRICARE MANAGEMENT ACTIVITY, http://www.tricare.mil/tma/AboutTMA.aspx (last visited Dec. 6, 2012).

[172] Bob Brewin, *Contractor Hit with Second Class Action Suit Over Tricare Data Theft*, NEXTGOV (Jan. 6, 2012), http://www.nextgov.com/health/2012/01/contractor-hit-with-second-class-action-suit-over-tricare-data-theft/50411/.

Washington D.C.[173] Of particular concern to the existence of actual harm and the possible calculation of damages is the fact that after the breach, TRICARE initially stated that they would not be providing credit monitoring services because they viewed the risk of financial harm as low.[174] Later, TRICARE changed their stance on this decision and directed SAIC to provide credit monitoring.[175]

The California suit has been filed on behalf any of the 4.9 million patients that currently live in California.[176] The suit alleges three causes of action: violation of security requirements for consumer records under the Information Practices Act of 1977, common law negligence, and common law invasion of privacy.[177] The plaintiffs seek actual damages, to be proven at trial, for "credit monitoring and insurance, out of pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm."[178] It seems unlikely that this will be granted class certification because invasion of privacy may present a "common question of fact" issue that is particularized to each plaintiff. Moreover, actual damages may be limited to credit monitoring services purchased before TRICARE directed SAIC to begin offering them, otherwise plaintiffs would have failed to mitigate their damages.

As stated, SAIC has been sued in a Texas federal court as well, in a suit that is also still pending.[179] This suit alleges that the class size includes all of the 4.9 million persons affected by

---

[173] *Id.*
[174] *As TRICARE Breach Case Illustrates, Credit Services Can Be a Very Contentious Issue*, 12.2 REPORT ON PATIENT PRIVACY (Feb. 13, 2012), *available at* http://aishealth.com/archive/hipaa0212-03. This also gravely understates the value of medical data, in comparison to financial data.
[175] Press Release, TRICARE Management Activity, *2011 SAIC Data Breach Statement and Q&A*; *available at* http://www.rucker.amedd.army.mil/assets/documents/pdf/SAIC_TRICARE_%20Breach%20Statement-QA_final_11_18.pdf.
[176] Class Action Complaint at 3, Losack v. SAIC, Inc., (Cal. Super. 2011) 37-2011-00102318-CU-MT-CTL, *available at* http://www.contractormisconduct.org/ass/contractors/47/cases/1767/2639/saic-losack_complaint.pdf.
[177] *Id.* at 8-10.
[178] *Id.* at 10.
[179] First Amended Class Action Complaint and Jury Demand at 1, Arellano v. SAIC, Inc., (W. TX. 2011) 5:11-cv-884-FB, *available at* http://www.govexec.com/pdfs/010512bb1b.pdf.

the breach.[180] Unlike other medical data cases, the plaintiffs allege a violation of the Fair Credit Reporting Act, either willfully or negligently, stating that SAIC is a Consumer Reporting Agency under the statute.[181] The Act has similar privacy requirements to HIPAA, and the plaintiffs claim that there was a duty to adopt protective procedures that would have thwarted the theft of the computer tapes and could result in actual damages between $100 and $1,000 per class member.[182] On top of these claims the plaintiffs have also asserted causes of action for negligence, invasion of privacy, and violation of the Texas Deceptive Trade Practices-Consumer Protection Act.[183] Like the class action in California, the plaintiffs may have trouble calculating actual damages that stemmed from the breach, especially after the credit monitoring services were offered.

The last and most recently filed of this trio of actions was brought against TRICARE and the Department of Defense in the District Court in the District of Columbia, also representing all 4.9 million consumers.[184] This action includes sub-classes representing plaintiffs of 24 different states.[185] The suit brought nine federal causes of action, including violations of the Administrative Procedures Act, Privacy Act of 1974, and Fair Credit Reporting Act, among others.[186] The suit then brings a number of state-specific causes of action for the sub-classes.[187]

While the three TRICARE cases may face dismissal for failure to state a claim upon which relief can be granted, an 11th Circuit appellate ruling may have given victims of medical

---

[180] *Id.* at 10.
[181] *Id.* at 13-15.
[182] *Id.* at 14. *See also* 15 U.S.C. § 1681n(a)(1)(A).
[183] *Id.* at 16-18.
[184] Consolidated Amended Class Action Complaint at 1, In re SAIC Backup Data Theft Litigation, (D.D.C. 2012), Misc. Action No. 12-mc-347 (RLW) MDL No. 2360, *available at* http://www.coffmanlawfirm.com/sites/www.coffmanlawfirm.com/themes/CoffmanRichard/pdf/18%20-%20Consolidated%20Amended%20Complaint%2010.01.2012.pdf.
[185] *Id.* at 57-64.
[186] *Id.* at 67-75
[187] *Id.* at 76-103.

data breach the greatest chance of recovery.[188] In December 2009, two unencrypted laptops were stolen from the corporate offices of AvMed Inc. in Gainesville, Florida resulting in a breach of 1.2 million health plan members.[189] One of the distinguishing aspects of this case is that two of the plaintiffs were victims of actual identity theft in the year following the breach, as their information was used to open a bank account and a brokerage account that were then overdrawn.[190] These plaintiffs were designated as a sub-class in the complaint.[191]

A Florida district court had ruled that the plaintiffs failed to state a cognizable injury, but the 11th Circuit Appellate Court overturned the dismissal allowing the case to go to trial.[192] The court held that actual identity theft is an injury in fact, and that it was fairly traceable to the breach.[193] The plaintiffs must still face class certification now that the case has been remanded; and if it reaches trial, it would be the first health data breach to do so in a federal court.[194] It may hurt the class's chances that only two plaintiffs have alleged actual identity theft, but the Appellate Court also overturned a motion to dismiss on a claim of unjust enrichment, holding that sufficient facts have been pleaded.[195] The complaint states that the monthly premiums paid to AvMed constitute a benefit conferred and should be recoverable because part of that premium was to go to data security.[196] Finding that the class has standing in a federal court may allow for the first trial over a medical data breach.

---

[188] Marianna Kolbasuk McGee, *Breach Class Action Suit Advances*, DATA BREACH TODAY (Sept. 19, 2012), http://www.databreachtoday.com/breach-class-action-suit-advances-a-5126.
[189] *Id.*
[190] *Id.*
[191] First Amended Class Action Complaint at 22, Resnick v. AvMed, Inc., 2011 WL 1188356 (S.D. Fla.).
[192] Resnick v. AvMed, Inc., 693 F.3d 1317, 1321 (11th Cir. 2012).
[193] *Id.* at 1323-1324.
[194] Marianna Kolbasuk McGee, *Breach Class Action Suit Advances*, DATA BREACH TODAY (Sept. 19, 2012), http://www.databreachtoday.com/breach-class-action-suit-advances-a-5126.
[195] Resnick v. AvMed, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012).
[196] *Id.*

If any of these class action suits were to go to trial or result in a significant settlement against a covered entity there would be substantial ramifications to HHS's enforcement of the Breach Notification Rule, the Privacy Rule, and the Security Rule. This would take enforcement out of the hands of governmental regulating bodies and give it to the private sector. A public policy concern that this may have is that monetary damages against covered entities will deter innovation in health information technology. Outside of the "meaningful use" incentives, a practice could decide to rely solely on paper records and take the most basic steps in preventing breach. On the other hand, a private cause of action could be very beneficial in deterring health data breaches. Once a breach is disclosed, HIPAA violations could be uncovered on discovery and the costs of litigation and/or settlement would not be placed on the government, so a lack of resources would no longer be an excuse. Of course, there would have to be some sort of limitations on these claims. A federal cause of action, preempting state claims, would eliminate much of the current confusion. Conversely, it would be unreasonable to expect a covered entity like TRICARE, who performs a public service, to payout $4.9 billion in damages following a breach. While there may be no right answer as to the proper amount of a statutory cap on damages, it would need to be greater than the current limit under the Breach Notification Rule and prosecuted with more regularity and consistency, in order to properly deter breaches.

VII. Additional Proposals to Quell Data Breaches

While a private cause of action may be the most fiscally daunting means of deterring the number of health data breaches, there are additional regulations that could be considered to keep breaches from occurring. Among these are amendments to the current Breach Notification Rule that would increase security regulations and an enhancement to the current HHS/OCR auditing system of covered entities.

A. Al Franken's Protect Our Health Privacy Act

Al Franken is the Senate representative for the state of Minnesota and the Chairman of the Subcommittee on Privacy, Technology, and Law.[197] Franken has addressed the insufficiency of the current laws, and specifically the lack of enforcement by HHS.[198] A panel discussion before the subcommittee partly attributed this to an inadequacy of regulations, most notably the delay in the issuing of a final HITECH rule.[199] While the panel did not come to any definitive resolutions, Franken has introduced a bill to the Senate to amend the current rule, called the Protect Our Health Privacy Act.[200]

The bill, which has been submitted to a committee for review, would require additional reports on complaints of health data breaches and how HHS and state attorney generals handle the complaints.[201] The reports would detail the number of informal resolutions and instances of declined enforcement in relation to the number of settlements and fines.[202] The purpose of this is to determine if HHS is enforcing the rule to the best of their ability and to see if there are areas in need of improvement.

In addition, the bill would expressly include portable media under the encryption rule, requiring the data to be "unusable, unreadable, or indecipherable to unauthorized individuals.[203] This would be an attempt to reduce the number of breaches that result from lost or stolen laptops. Lastly, the bill would extend federal regulations governing covered entities to business

---

[197] Rachel Grunberger, *Senate Hearings Focus on Lack of HIPAA Enforcement, Final HITECH Rule*, INSIDEPRIVACY (Dec. 22, 2011), http://www.insideprivacy.com/senate-hearings-focus-on-lack-of-hipaa-enforcement-final-hitech-rule/.
[198] *Your Health and Your Privacy: Protecting Heath Information in a Digital World: Hearing Before the Subcomm. On Privacy, Technology, and the Law*, 112th Cong. (2011), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=9b6937d5e931a0b792d258d9b332c04d.
[199] *Id.*
[200] Protect Our Health Privacy Act, S. 3351, 112th Cong. (2012).
[201] *Id.* at § 2.
[202] *Id.*
[203] *Id.* at § 3.

associates, as well as requiring that agreements between the two must limit the scope of use of the data to only that which is necessary for the performance of the function.[204] Although the bill does not increase monetary penalties or regulation, it may at least put covered entities on notice of the regulations and be the stepping stone for the release of a final HITECH rule.

B. Auditing

A final means of ensuring compliance of the Security and Privacy Rules and reducing the number of health data breaches would be to increase the amount of auditing of covered entities and business associates. HITECH provides HHS with a statutory grant to perform periodic audits.[205] OCR has undertaken the duty of performing the audits and began a pilot program in November 2011.[206] HHS proclaims the audits to be "comprehensive" in scope of the investigation, but OCR only audited 115 covered entities in the first year of the pilot program.[207]

One potential way of increasing the number of and effectiveness of audits is to develop a covered entity-to-covered entity auditing program. This could require health IT employees and/or administrators to travel to other covered entities and perform an audit based on HHS guidelines. This audit could then be submitted to HHS, who could determine whether or not to further investigate covered entities after negative audits. An entity based auditing system would increase the total number of covered entities that are inspected and require the entities to be in compliance with the mandatory federal regulations.

Another possible auditing system that would ensure that entities are being inspected properly would be to require accreditation from a third party auditor. Covered entities could be

[204] *Id.* at § 4.
[205] 42 U.S.C. § 17940.
[206] *HIPAA Privacy & Security Audit Program*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html (last visited Dec. 6, 2012).
[207] *Id.*

required meet a certain standard, such as the gold standard from The Joint Commission.[208] This could then be tied to government kickbacks, like those related to "meaningful use." An auditing system like this is more likely to ensure compliance than the risk of facing monetary penalties following a breach of health data.

CONCLUSION

As HITECH "meaningful use" requirements push more health data records into ePHI, patients become more and more susceptible to data breach. This issue has been recognized by the HHS and OCR, but not properly addressed or enforced. The number of large-scale data breaches has grown to over 500 since the Breach Notification Rule was signed into law. While the Rule takes the first step in making patients aware of potential privacy concerns, it has not done enough to stop the breaches from happening.

In order to reduce the number of breaches, HHS must make known to covered entities and business associates that breaches will not be taken lightly, especially when there are additional privacy and security violations. Plaintiffs have faced a substantial amount of resistance in bringing private claims under state laws and a federal, private cause of action under the Breach Notification Rule could resolve much of the current confusion. Another way of reducing the number of breaches would be to increase enforcement of the Federal Regulations. Unfortunately, this is not a top priority for HHS, or may be beyond their means, and this could be addressed through the implementation of a more structured auditing system. Entity-to-entity auditing or accreditation auditing systems would take much the enforcement costs from HHS and place it in the hands of the entities, while ensuring greater compliance. While there may be no

[208] *What is Accreditation?*, THE JOINT COMMISSION , http://www.jointcommission.org/accreditation/accreditation_main.aspx (last visited Dec. 6, 2012).

guaranteed way reducing health data breaches, a mixture of these proposals would surely go to benefit patient privacy in the future.