

2014

# Hacking Health Care: Authentication Security in the Age of Meaningful Use

Gordon Gantt Jr.

# HACKING HEALTH CARE: AUTHENTICATION SECURITY IN THE AGE OF MEANINGFUL USE

GORDON GANTT, JR.*



## I. INTRODUCTION

In the summer of 2012, at a small surgical practice located outside of Chicago, an employee tried to log into the practice's secure server, but instead was greeted by an odd message.[1] The message stated that the data on the server, which included thousands of individual electronic health records and confidential emails, had been encrypted and could only be accessed by a password.[2] That password would be provided, the message explained, for a fee.[3]

On June 25, 2012, the Surgeons of Lake County, located in Libertyville, Illinois, became one of the latest victims of a growing phenomenon: electronic health record extortion.[4] The ploy is simple. A hacker gains access to a large store of personal medical records on a "secure" server.[5] The hacker simply removes or encrypts the

* Gordon R. Gantt, Jr. graduated from Cleveland-Marshall College of Law in May 2014. He also holds a Bachelors of Arts degree in Journalism from the Ohio State University. He wishes to thank his family, Prof. Gwendolyn Majette, and his wife Luisa for their endless encouragement and support.

[1] Press Release, Surgeons of Lake Cnty., LLC, Incident Triggers Investigation as to Whether Patient Information May Have Been Improperly Accessed (July 20, 2012), *available at* http://www.send2press.com/newswire/2012-07-0720-001.shtml.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

data, then holds it for ransom.[6] The thief does not break windows, kick in doors, or even have to leave the comfort of his own home. While sophisticated extortion scams are still rare,[7] they are sober reminders of the vulnerability of the highly valuable and personal information patients share with their health care providers.

Over the last few years, adoption of electronic health records (EHRs) increased.[8] In part, this is a result of increased pressure by regulators to adopt EHR technology to improve the efficiency and quality of medical care.[9] In years to come, Medicare and Medicaid reimbursement will be determined in part by the provider's use or non-use of EHR.[10] In the twenty-first century, it seems unlikely that government incentives would be necessary to spark interest in adopting new technology, but the health care industry lags behind other industries in terms of electronic records utilization.[11] This is in part because of the unique character of the information contained in medical records. Protected Health Information (PHI) carries a substantial privacy interest because EHRs hold vast amounts of personal information; not only is a patient's private medical history at risk, but names, addresses, birth dates, and social security numbers in electronic form are also vulnerable.[12] That private data is collected with thousands, sometimes millions, of other patient records onto a single server.[13] Many healthcare providers were reluctant to place electronic Protected Health Information (ePHI) in what they perceived to be the vulnerable, virtual realm.[14] Ironically, this delay in conversion might have made ePHI even more susceptible.

---

[6] *Id.*

[7] Neil Versel, *Cyber Crooks Target Healthcare for Financial Data*, INFO. WK. (Oct. 24, 2012), http://www.informationweek.com/healthcare/security-privacy/cyber-crooks-target-healthcare-for-finan/240009668.

[8] Eric Jamoom et al., *Physician Adoption of Electronic Health Record Systems: United States, 2011*, http://www.cdc.gov/nchs/data/databriefs/db98.htm (last visited Feb. 15, 2014).

[9] *Health IT Regulations Meaningful Use Regulations*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/meaningful-use-regulations (last visited Aug. 4, 2014).

[10] *Id.*

[11] Julie Gray, *Modernizing Healthcare Communication: Medical Information When and Where You Need It*, PEORIA MAG. (Feb. 2010), http://www.peoriamagazines.com/ibi/2010/feb/modernizing-healthcare-communication.

[12] *What is the Difference Between a Personal Health Record, an Electronic Health Record, and an Electronic Medical Record?*, HEALTHIT.GOV, http://www.healthit.gov/patients-families/faqs/what-difference-between-personal-health-record-and-electronic-health-record-a (last visited Aug. 4, 2014).

[13] *See generally Breaches Affecting 500 or More People*, HEALTHIT.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breach tool.html (last visited Aug. 4, 2014).

[14] Vince Kuraitis, *Overcoming the Penguin Problem: Setting Expectations for EHR* Adoption, E-CARE MGMT. BLOG (Aug. 2, 2009), http://e-caremanagement.com/overcoming-the-penguin-problem-setting-expectations-for-ehr-adoption/. Another issue, which compounds the practical concerns, is the "penguin problem" that Kuraitis focuses on in this article. The penguin problem is an economic phenomenon in which everyone in a given population waits for someone to be the first to adopt a new method or technology, so no one adopts the new

As the health care industry plays catch-up, it runs the risk of advancing too quickly and falling prey to a highly sophisticated population of hackers. While providers may feel the sting of regulators for failing to keep up with rapidly advancing online security norms, it is the patients that are the real victims. The breach at the Surgeons of Lake County was relatively small.[15] Only a little over 7,000 patient records were compromised in that case.[16] But the numbers can run much higher. In March and April 2012, hackers breached the Utah Department of Health servers and gained access to roughly 800,000 individual electronic health records.[17]

The rapid adoption of EHRs, to store and communicate highly personal data, raises serious concerns in terms of privacy, security, and civil and criminal liability. This note will examine the current statutory framework for addressing electronic breaches in the health care context, examine the vulnerabilities of EHRs, and look to the established world of online banking for possible legislative and practical solutions to the challenge of keeping private health information private. Finally, this note will propose key amendments to the Health Insurance Portability and Accountability Act (HIPAA) regulations to enhance authentication security.

## II. BACKGROUND

Medical records are the principal repository for a patient's health and health care history.[18] Traditionally, these records were paper documents that were passively used by providers for historical reference.[19] EHR technology provides capabilities and improved efficiencies that paper records could never achieve.[20] The ability to share patient information contained in EHRs promises to revolutionize the practice of medicine by turning what was once a historical reference into a tool that can proactively prevent harmful drug interactions and allergies, reduce the chances that a clinician's orders will be misread or illegible, and facilitate the coordination of care across multiple providers.[21]

The many benefits of EHR technology are inherently counterbalanced by the increased threat to patient privacy. As one scholar put it, "[a]s society has progressed and grown to new digital heights . . . it also has become more vulnerable to

---

method or technology. Kuratsis suggests that this phenomenon is a reason for the health care industry's slow adoption of EHR technology.

[15] *Health Information Privacy for the Surgeons of Lake County*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotification rule/breachtool.html (last visited Aug. 4, 2014) (search "Surgeons of Lake County;" enter for state "Illinois;" then apply filter).

[16] *Id.*

[17] *See* HEALTHIT.GOV, *supra* note 13; *see also*, Patty Henetz, *Utah Health Dept Chief: Hacked Data Stored Too Long*, SALT LAKE TRIB. (May 3, 2012), http://www.sltrib.com/sltrib/ news/54037017-78/health-security-department-patton.html.csp.

[18] Eric S. Pasternack, *HIPAA in the Age of Electronic Health Records*, 41 RUTGERS L.J. 817, 818 (2010).

[19] *Id.*

[20] *Id.* at 819.

[21] *Id.*at 819–21.

unwanted intrusions of privacy."[22] These intrusions negatively impact patient confidence in their providers' ability to secure their private data.[23] A survey by the National Partnership for Women and Families found that fifty-nine percent of patients who see a doctor that uses EHR technology feel that widespread adoption of EHR technology will lead to more personal information being lost or stolen.[24]

The level of trust and comfort a patient has with his clinician has a direct relationship with the quality of care the patient receives.[25] A breach of trust between a patient and clinician can result in irreparable physical harm to the patient.[26] The amount of information a patient is willing to disclose to his or her clinician can impact the accuracy of diagnoses and the course of treatment recommended.[27] Thus, patient/clinician trust is not just beneficial to quality care, but essential.

### *A. The Role of HIPAA*

Congress recognized the importance of patient information security to health care through the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[28] Despite its nebulous label, HIPAA's most well-known provisions address the privacy and security of patient health information (PHI).[29] The HIPAA privacy rule has three major purposes:

> 1. To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information; 2. To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and 3. To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.[30]

These purposes are achieved by establishing a demanding federal standard for the electronic maintenance and storage of PHI.[31] The Act applies only to "covered

---

[22] Varick D. Love, *Privacy Ethics in Health Care*, J. HEALTH CARE COMPLIANCE, July–Aug. 2011, at 15.

[23] *Id*. at 17.

[24] Press Release, Nat'l P'ship for Women & Families, Making IT Meaningful: How Consumers Value and Trust Health IT is Unprecedented (Feb. 15, 2012), *available at* http://www. nationalpartnership.org/news-room/press-releases/with-government-providing.html.

[25] Audiey C. Kao et al., *Patients' Trust in their Physicians*, 13 J. GEN. INTERNAL MED. 681 (1998), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1500897/.

[26] Love, *supra* note 22, at 17.

[27] *Id.*

[28] Pasternack, *supra* note 18, at 818.

[29] *Id.*

[30] *Id.* at 825 n.71.

[31] *Id.*

entities" which include health plans, health care clearinghouses, and health care providers that transmit PHI in electronic form.[32] The general rule set forth by HIPAA is that covered entities must obtain patient authorization before releasing PHI. However, this otherwise simple rule is complicated by numerous exceptions that permit, or even compel, disclosure, even in the absence of such authorization.[33] Notably, HIPAA does not provide patients with a private cause of action for unlawful disclosure of PHI, but is instead enforced through civil and criminal proceedings originated by the Department of Health and Human Services and the Department of Justice.[34]

Given the narrow scope and limited remedies provided in HIPAA, it has been criticized for focusing too much on patient consent and ignoring the technological realities presented by a growing number of non-covered entities that maintain electronic PHI.[35] These criticisms may explain why Congress took additional action in 2009 through the Health Information Technology for Economic and Clinical Health Act (HITECH).[36]

### *B. HITECH Amendments to HIPAA*

HITECH had two overarching purposes: (1) to incentivize the adoption of health information technology, including EHRs, and (2) to increase the privacy and security protections originally provided in HIPAA.[37] To this end, HITECH makes federal funds immediately available to providers to help pay for EHR technology and to conduct training and education to develop the "best practices" of EHR utilization.[38] On the security side, the Act obligates covered entities to disclose breaches of EHRs to the individuals affected.[39] A breach occurs when unsecured PHI is acquired,

---

[32] *Id.* at 826–27.

[33] *Id.* at 827.

[34] *Id.* at 828, 831–38, 840–41. While HIPAA does not expressly provide a private cause of action, it has been successfully used for establishing a standard of care in tort claims for invasion of privacy, breach of privacy, and negligent infliction of emotional distress. *See* Acosta v. Byrum, 638 S.E.2d 246, 253 (2006).

[35] Pasternack, *supra* note 18, at 827.

[36] *See generally* HITECH Act, 42 U.S.C. §§ 300jj, §§ 17901 (2012).

[37] Lisa L. Dahm, *Carrots and Sticks in the HITECH Act: Should Covered Entities Panic?*, 22 HEALTH LAW 1 (Aug. 2010).

[38] *Id*. at 3.

[39] *Id* at 4. As Dahm explains, once a covered entity discovers that a breach has occurred, it must notify the individuals whose PHI is involved "without unreasonable delay and in no case later than 60 [sixty] calendar days." Notice must be provided in writing and sent via first-class mail to each individual's last known address and must include:

> (1) A brief description of what happened, including the date of breach and the date of the discovery of the breach, if known; (2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code); (3) The steps individuals should take to protect themselves from potential harm resulting from the breach; (4) A brief description of what the covered entity involved is doing to investigate the breach, mitigate losses, and protect against any further breaches; (5) Contact procedures for individuals to ask questions or learn additional

accessed, used, or disclosed by an unauthorized individual and the privacy or security of the PHI is, or may be, compromised.[40] HITECH also requires covered entities' business associates to comply with HIPAA security regulations.[41]

HITECH still does not provide for a private cause of action to those affected by data breaches; however, it does permit a state attorney general to bring a civil action on behalf of state residents to enjoin a violation of HITECH and to obtain statutory damages on behalf of affected residents.[42] Generally, while HITECH provides some enhanced penalties[43] and expands liability under the act to business associates and employees of covered entities, the Act is still narrowly tailored and forces affected individuals to rely on action by federal and state regulators to seek remedies for breaches of EHRs.[44]

### *C. HIPAA: The Final Rule*

On January 17, 2013, the Department of Health and Human Services released the long-awaited HIPAA final rule.[45] The new rule officially adopted many of the changes called for in HITECH and the Genetic Information Non-Discrimination Act of 2008.[46] According to HHS, the final rule "greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law".[47] The final rule became effective on March 23, 2013, but covered entities and their business associates had until September 23, 2013, to come into full compliance with its new requirements.[48]

Among the final rule's most prominent features is the complete replacement of the Breach Notification rule as set forth in the interim final rule, the extension of

---

information, which shall include a toll-free telephone number, an email address, web site, or postal address. *Id.*

[40] *Id.*

[41] *Id.*

[42] *See* HITECH Act, Section 13410(e)(1)(codified at 42 U.S.C. § 17939(e)(1) (2012)).

[43] *See* HITECH Act, Section 13410(a) (codified at 42 U.S.C. § 17939(a) (2012)).

[44] Devin D.Vinson, *No More Paper Tiger: Promise and Peril as HIPAA Goes HITECH*, 30 J. HEALTHCARE RISK MGMT. 28 (2011).

[45] Press release, U.S. Dep't of Health and Human Servs. New rule protects patient privacy, secures health information (Jan. 17, 2013), *available at* http://www.hhs.gov/news/press/2013pres/01/20130117b.html. A final rule is obtained after a proposed rule is put forth by a regulatory agency. Proposed rules are subjected to public comment from a variety of stakeholders. Those public comments are reviewed by the administrative agency and any suggestions for modification of the rule contained in those comments are considered and sometimes adopted in the final rule.

[46] *Id.* The Genetic Information Non-Discrimination Act of 2008 (GINA) provides individuals with increased protection against disclosure of genetic information and specifically prohibits the use or disclosure of genetic information by health insurers for underwriting purposes. Final rule provisions related to GINA do not alter or add to technical security safeguards and thus are not relevant to this article.

[47] *Id.*

[48] *Id.*

liability for breaches to business associates and the dramatic increase in civil monetary penalties.[49] The final rule provides the following summary of its major provisions:

> "This omnibus final rule is comprised of the following four final rules:
> 1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:
>
> Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.
>
> Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
>
> Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
>
> Require modifications to, and redistribution of, a covered entity's notice of privacy practices.
>
> Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
>
> Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule (referenced immediately below), such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.
>
> 2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.
> 3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's "harm" threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.
> 4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009."[50]

## III. DISCUSSION

HIPAA seems far removed from the practical realities of modern EHR utilization. While attacks on health care entities are still relatively rare, hackers are

---

**49** 78 C.F.R. § 5566 (2013).

**50** *Id.*

stealing ePHI at an ever increasing rate, leaving patients vulnerable to identity theft and, perhaps more importantly, loss of control over highly sensitive Protected Health Information.[51] The threat posed by hackers is a symptom of institutional security failure.[52] Hackers gain access to PHI through system vulnerabilities.[53] As a security issue, examination of these issues requires careful analysis of the HIPAA Security Rule and, more specifically, the technical standards it requires. In order to understand how to better protect ePHI, it is first necessary to understand the nature of the threat and the current required safeguards. The remedy will be found where current safeguards fail to address the threat.

### *A. The Nature of the Threat*

In recent months, the Department of Homeland Security ("DHS") has expressed concerns that the health care systems present an inviting target to activist hackers, cyber warriors, criminals, and terrorists.[54] DHS has found that the same type of trivial security flaws which hackers have exploited in the financial, defense, and private business sectors still exist in the health care industry and are going uncorrected.[55]

Not only are there a swarm of foreign and domestic hackers threatening all forms of electronic data, but there are several new ways to remotely access that data.[56] Cell phones, laptops, and tablets have become popular tools in the health care field.[57] For example, the Apple iPad features an electronic charting application called

---

[51] Robert O'Harrow, Jr., *Health-Care Sector Vulnerable to Hackers, Researchers Say*, WASH. POST (Dec. 25, 2012), http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html (This article was the culmination of a year-long investigation by the *Washington Post*. The investigators determined that the health care industry is among the most vulnerable industries in terms of cyber security. Avi Rubin, a computer scientist and technical director of the Information Security Institute at Johns Hopkins University, told the *Washington Post* "[i]f our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed.").

[52] *Id.*

[53] HEALTHIT.GOV, U.S. DEP'T OF HEALTH AND HUMAN SERVS., GUIDE TO PRIVACY AND SECURITY OF HEALTH INFORMATION 13, http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

[54] *Id.*

[55] *Id.*

[56] *See* Abigail Philips, *Microsoft Surface Enters mHealth Market*, HEALTHCARE GLOBAL (Feb. 26, 2013), http://www.healthcareglobal.com/healthcare_technology/microsoft-surface-enters-mhealth-market; *see also* Scott Mace, *How Tablets are Influencing Healthcare*, HEALTH LEADERS MEDIA (March 6, 2013), http://www.healthleadersmedia.com/page-2/TEC-289831/How-Tablets-are-Influencing-Healthcare.

[57] *See* Eric Wicklund, *mHealth in the Exhibit Hall: It's No Longer All About the Shiny New Toys*, HEALTHCAREIT NEWS (Mar. 5, 2013), http://www.healthcareitnews.com/news/mhealth-exhibit-hall-its-no-longer-all-about-shiny-new-toys; *see generally* Susan Standing & Craig Standing, *Mobile Technology and Healthcare: The Adoption Issues and Systemic Problems*, 4 INT'L J. ELECTRONIC HEALTH CARE 221, 221–35 (2008), *available at* http://inderscience.metapress.com/content/071725p701448111/.

"DrChrono" which its developer claims meets Stage-1 Meaningful Use under HITECH.[58] The application allows providers to transmit medical billing information, transmit electronic prescriptions, and share EKG, X-Ray, and lab results all from the iPad.[59] These portable devices are certainly more convenient and provide users with numerous benefits that have the potential to improve the quality of care, but as soon as these devices come out hackers develop new ways to subvert their security measures.[60] The answer can't be to abandon these new technologies, but rather to make them more secure with improved security standards that are already implemented in other industries.

While it is nearly impossible to stop a sophisticated hacker who is determined to gain access to a healthcare network, many of the current security practices in place are so sub-standard that even a hacker with relatively low-skill can gain access. The University of Chicago Medical Center, for example, found that multiple resident physicians were using a single password to access an online dropbox used to manage patient care.[61] Worse still, the password was published in an online manual.[62] After the media brought the vulnerability to the medical center's attention, it took steps to resolve the problem.[63] Unfortunately, the Office of Civil Rights website is filled with examples of such vulnerabilities which are being discovered too late.[64]

Even by curing this low hanging fruit through improved administrative security measures, the threat from more sophisticated attacks remains. In the Information Age, these threats come from around the globe.[65] They can even be highly coordinated among multiple hackers as demonstrated by the now famous hacking organization known as "Anonymous" which uses social media and websites to plan large scale attacks on various businesses, groups, and governments.[66]

Protecting ePHI from these hackers is a constant technological arms race. As quickly as new cutting edge barriers are put up, someone is figuring out how to tear

---

[58] *See* DRCHRONO INC., https://drchrono.com/ipad_ehr/ (last visited March 7, 2013).

[59] *Id.*

[60] *See, e.g.*, Nate Hoffelder, *Got 5 Seconds? Why Not Hack an IPad 2*, MEDIA BISTRO (Oct. 24, 2011), http://www.mediabistro.com/appnewser/got-5-seconds-why-not-hack-an-ipad-2_b17008.

[61] O'Harrow, *supra* note 51.

[62] *Id.*

[63] *Id.*

[64] The HIPAA final rule, published by HHS on January 18, 2013, incorporates the HITECH Act's mandatory breach notification for breaches of ePHI that affect 500 or more patients. A running list of these breaches is published in accordance with section 13402(e)(4) of the HITECH Act and is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[65] *Cyber Threat Warnings Grow Louder*, FCW (Aug. 15, 2012), http://fcw.com/articles/2012/08/15/buzz-cyber-threat.aspx?m=2.

[66] James Schmidt, *What is 'Anonymous'?,* EXAMINER.COM (Jan. 14, 2013), http://www.examiner.com/article/what-is-anonymous.

them down.[67] At the same time healthcare IT professionals are trying to keep unauthorized users out, there is a growing trend toward making electronic medical records available to patients online.[68]

### *B. The Value of the Threatened Information*

Part of the reason ePHI is so sensitive is that it may contain details about a person's health history and that information might be embarrassing or be perceived to negatively impact the person's ability to gain employment or insurance, but one of the primary reasons hackers target EHRs is for financial information.[69] Hackers are looking for information from which they can directly or indirectly profit.[70] HIPAA provides a detailed list of the sort of information that must be removed or redacted from EHRs in order to consider the record "de-identified."[71] De-identification is not at issue in this note, but the list does illustrate the range of information often found in EHRs. The list includes:

> (A) Names;
> (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
> (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
> (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
> (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
> (D) Telephone numbers;

---

[67] Richard Barber, *Managing X-Commerce: The Importance of a Security Based Architecture When Preparing for E-Commerce*, May 2001, at 9–12, *available at* http://www.sciencedirect.com/science/article/pii/S1353485801005141#.

[68] *See* Pasternack, supra note 18; *see also* Steve Lohr, *Google to End Health Records Service After it Fails to Attract Users*, N.Y. TIMES (June 24, 2011), http://www.nytimes.com/2011/06/25/technology/25health.html?_r=0. Google Health was a major attempt by a prominent developer to provide patients with online access to ePHI. Launched in 2008, the goal of the service was to translate their consumer-centered approach, which was successfully applied to other domains, to the health care industry and to impact the day-to-day health experiences of its users. Despite nearly three years of effort and the strength of its brand, Google Health was abandoned in the beginning of 2012. The complexity of the service and the laborious task of putting health information into the system discouraged wide adoption, and the service failed to have the large impact the company had envisioned. Still, it seems inevitable that consumer-driven EHRs will find a place in the market and become as ubiquitous as online banking.

[69] Versel, *supra* note 7.

[70] 45 CFR § 164.514(d)(2)(i) (2013).

[71] *Id.*

(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section;

Valuable financial data is often what draws hackers to healthcare records, but health and financial information is often not segmented from other types of information.[72] In other words, patients who have their EHRs hacked run the risk of not only having their identity stolen, but also of having their private medical history compromised. The value of personal medical history extends even beyond the individual whose ePHI has been exposed by a breach due to the genetic information that can often be found in those records.[73]

### *C. HIPAA Security Requirements*

In this fast moving environment, slow-moving and narrowly tailored regulation is a poor defensive strategy. Instead, HHS created rules based on the fundamental concepts of flexibility, scalability, and technology neutrality.[74] HIPAA does not identify specific security measures to implement, but a covered entity is permitted to use any security measures that allow it to "reasonably and appropriately" implement

---

[72] Versel, *supra* note 7.

[73] Kristen Carl, *It's Personal: Privacy Concerns Associated with Personal Health Records*, 5 I/S: A J. L. & POL'Y FOR THE INFO. SOC'Y 533 (2010). As Carl elucidates,

> [m]edical records arguably contain a person's most sensitive and private information. Because many medical conditions are hereditary, a single medical record may include equally sensitive information about countless other individuals. The damaging effects brought on by a breach in the security of this information are endless. Third parties - employers, bankers, neighbors - could use this information to discriminate against and potentially ostracize an individual diagnosed with an "unpopular" disease or condition. With the development and rising popularity of the online "personal health record" through mediums such as Google Health and Microsoft HealthVault, two important questions arise: (1) is storing medical information online safe and securely protected; and, (2) in the event of a breach, whom does the law hold accountable?

*Id.*

[74] U.S. Dep't of Health & Human Services, *Security Standards: Technical Safeguards*, HIPAA SECURITY SERIES, May 2005 (rev. March 2007), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

the standards and implementation specifications.[75] These regulations are set forth in the HIPAA Security Rule.[76] Whether a particular measure is "reasonable and appropriate" is determined through a multi-factor analysis provided in the security rule.[77] The factors include:

> (i) The size, complexity, and capabilities of the covered entity.
> (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
> (iii) The costs of security measures.
> (iv) The probability and criticality of potential risks to electronic protected health information.[78]

HIPAA appears to, and was in fact designed to, permit substantial discretion on the part of the covered entity in determining what specific measures to take.[79] Of course, once a breach occurs this lack of direction makes the covered entity's task of defending its security measures that much more complex and arbitrary.[80] If the covered entity is able to determine that it is subject to the required implementations based on this nebulous multi-factor test, then it must implement the equally

---

[75] *Id*.

[76] 45 C.F.R. § 164.306 (2013). This rule provides in relevant part:

> (a) General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits; (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.

[77] 45 C.F.R. § 164.306(b)(2) (2013).

[78] *Id.*

[79] 45 C.F.R. § 164.306(b) (2013).

[80] Farrokh Alemi, *Privacy and Confidentiality*, HEALTH SYSTEMS ADMIN., http://gunston.gmu.edu/healthscience/740/HIPAA.asp?E=0 (last visited Aug. 27, 2014).

enigmatic administrative,[81] physical,[82] and technical[83] safeguards as well as organizational,[84] policies, procedures, and documentation[85] requirements.

The administrative safeguards require the covered entity to conduct an "accurate and thorough" risk analysis.[86] Covered entities must then address those risks through

[81] 45 C.F.R. § 164.308 (2013) describes the administrative safeguards and implementation procedures a covered entity must enact including risk analysis, security management processes, sanction policies, information system activity reviews, and workforce security, among many others. 45 C.F.R. § 164.308 (2013). Consult 45 C.F.R. § 164.308 (2013) for a full list of requirements.

[82] 45 C.F.R. § 164.310 (2013) describes the physical safeguards and implementation procedures a covered entity must enact including facility access controls, device and media controls, disposal policies, and data backup and storage policies. 45 C.F.R. § 164.310 (2013).

[83] 45 C.F.R. § 164.312 (2013) describes the technical safeguards and implementation procedures a covered entity must enact including unique user identification, automatic logoff, emergency access procedures, and audit controls, among many others. 45 C.F.R. § 164.312 (2013) .

[84] 45 C.F.R. § 164.314 (2013) sets forth the organizational requirements for covered entities and their relationships with agents, employees, governmental entities, and other parties. 45 C.F.R. § 164.314 (2013).

[85] 45 C.F.R. § 164.316 (2013).

> A covered entity must, in accordance with § 164.306*:*
> (a) Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
> (b)(1) Standard: Documentation.
> (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and
> (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
> (2) Implementation specifications:
> (i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
> (ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
> (iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

45 C.F.R. § 164.316 (2013).

[86] 45 C.F.R. § 164.308(a)(1)(ii)(A) (2013). Specifically, the risk analysis is limited to potential vulnerabilities to the confidentiality, integrity, and availability of PHI. *Id.*

the implementation of "sufficient" security measures,[87] and apply an "appropriate" sanction policy to its workforce in the event of non-compliance with the covered entity's security policies and procedures.[88] Finally, the covered entity must conduct "regular" reviews of its information systems activity, including audit logs, access reports, and security incident tracking reports.[89]

Physical safeguards require the covered entity to limit access to electronic information systems to authorized users through policies and procedures regarding use and receipt and removal of electronically stored data, as well as physical safeguards.[90] Specifically, the covered entity must implement policies and procedures for disposal and removal of PHI prior to media re-use.[91]

The technical safeguards required of a covered entity include the access controls for ePHI, such as unique user identification and a procedure for obtaining access to ePHI in the event of an emergency.[92] Covered entities must also implement audit controls which record and examine user activity with ePHI[93] and policies and procedures which prevent the unauthorized alteration or destruction of PHI.[94] Person or entity authentication procedures are required to ensure that the person or entity seeking access is actually authorized.[95] Finally, the covered entity is required to implement technical safeguards to ensure the secure transmission of ePHI over a communications network.[96]

The organizational requirements under HIPAA require a contractual agreement between a covered entity and business associate.[97] The terms of that agreement bind the business associate to the same security and privacy standards as the covered entity.[98] Notably, under these organizational requirements the covered entity is

---

[87] 45 C.F.R. § 164.308(a) (2013). Sufficiency in this case is determined by the application of general requirements outlined in 45 C.F.R. § 164.306(a).

[88] 45 C.F.R. § 164.308(a)(1)(ii)(C) (2013).

[89] 45 C.F.R. § 164.308(a)(1)(ii)(D) (2013).

[90] 45 C.F.R. § 164.310(a)(1) (2013).

[91] 45 C.F.R. § 164.310(d)(2) (2013). An example of re-useable media is a re-writable compact disk or flash drive. In order for these items to be re-used, existing PHI must be removed to ensure existing ePHI is not needlessly disclosed when the media device is re-used.

[92] 45 C.F.R. § 164.312(a) (2013). Access control requirements under the technical safeguard provisions must limit access to those who are granted access rights as specified in 45 C.F.R. §164.308(a)(4).

[93] 45 C.F.R. § 164.312(b) (2013).

[94] 45 C.F.R. § 164.312(c)(1) (2013).

[95] 45 C.F.R. § 164.312(d) (2013).

[96] 45 C.F.R. § § 164.312(e)(1) (2013).

[97] 45 C.F.R. § 164.314(a)(1) (2013).

[98] *Id.* Under the Health Information Technology for Economic and Clinical Health Act of 2009, which amended HIPAA, a business associate of a covered entity is held to HIPAA standards regardless of the terms or even existence of a written agreement. This rule was also adopted in the HIPAA final rule released on Jan. 17, 2013. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the GINA, 78 Fed. Reg. 5566 (Jan. 25, 2013). The rule explains the analysis for determining if

considered to be in violation if the business associate breaches the contract by failing to meet those standards and the covered entity fails to take "reasonable" steps to cure that breach.[99]

Finally, the covered entity is required to implement certain policy, procedure, and documentation standards.[100] Consistent with the rest of the regulation, the policies and procedures implemented must be "reasonable and appropriate" for the covered entity to remain in compliance.[101] All policies and procedures must be documented and maintained for no less than six years from the date of their creation or the date when they were put into effect, whichever is later.[102] The documents must then be made available to the persons responsible for implementation and updated in response to any environmental and operational changes that affect the security of ePHI.[103]

---

an agent meets a business associate standard as follows, "[a]n analysis of whether a business associate is an agent will be fact specific, taking into account the terms of a business associate agreement as well as the totality of the circumstances involved in the ongoing relationship between the parties." Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the GINA, 78 Fed. Reg. 5566 (Jan. 25, 2013).

[99] 45 C.F.R. § 164.504(e)(1)(ii) (2013).

> (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful--
> (A) Terminated the contract or arrangement, if feasible; or
> (B) If termination is not feasible, reported the problem to the Secretary.

*Id.*

[100] 45 C.F.R. § 164.316 (2013).

[101] *Id*. The reasonableness is determined through the flexibility approach set forth in 45 C.F.R. § 164.306(b):

> (b) Flexibility of approach.
> (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
> (2) In deciding which security measures to use, a covered entity must take into account the following factors:
> (i) The size, complexity, and capabilities of the covered entity.
> (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
> (iii) The costs of security measures.
> (iv) The probability and criticality of potential risks to electronic protected health information.

45 C.F.R. § 164.306(b) (2013).

[102] 45 C.F.R. §§ 164.316(a)(1)(ii)–164.316(b)(2)(1) (2013).

[103] 45 C.F.R. § 164.316(b)(2) (2013).

The Security Rule measures paint a rough outline for covered entities to follow. That outline is further complimented by a myriad of so-called "addressable"[104] measures.[105] The addressable measures are not required unless an assessment by the covered entity reveals the measures to be "reasonable and appropriate"[106] in the entity's environment when analyzed with reference to the likely contribution to the protection of ePHI.[107] Among those "addressable" measures is the requirement to have ePHI encrypted whenever it is transmitted electronically.[108] The standard provided within the technical safeguard requirements is merely to implement "technical measures" to guard against unauthorized access of ePHI.[109]

When HITECH was unveiled as part of the American Recovery and Reinvestment Act of 2009, it provided additional actions by covered entities once a breach had occurred, but HITECH did not require the implementation of more rigorous initial security measures than were required originally under HIPAA.[110] Although, the new rules under HITECH did impose substantially harsher civil and criminal penalties for covered entities whose non-compliance results in breaches of ePHI.[111]

### *D. Federal Security Standards in the Financial Industry*

Electronic banking information carries a similar expectation of privacy to ePHI and can offer guidance in formatting a workable security standard. Like the health care industry, the financial industry requires the electronic storage and regular transfer of confidential information among various entities.[112] A key difference between the two industries is that the financial services industry is leaps and bounds ahead of the health care industry in terms of remote access and management of personal financial information.[113]

Online security standards in the financial services industry are promulgated by the Federal Financial Institutions Examination Council (FFIEC), an interagency council that is charged with producing standards and guidance for electronic financial data security.[114] FFIEC was created as part of the Federal Institutions

---

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] 45 C.F.R. § 164.306(d)(3)(i) (2013).

[108] 45 C.F.R. § 164.312(e)(2)(ii) (2013).

[109] 45 C.F.R. § 164.312 (2013).

[110] Howard Anderson, *HITECH Stage 2 Rules Unveiled*, DATA BREACH TODAY (Aug. 23, 2012), http://www.databreachtoday.com/hitech-stage-2-rules-unveiled-a-5060.

[111] 42 U.S.C. § 1320d-6 (2012); 45 C.F.R. § 160; 45 C.F.R. § 164.

[112] O'Harrow, *supra* note 51.

[113] *Id.*

[114] Paul Rice, *Civil Liability Theories For Insufficient Security Authentication in Online Banking*, 10 DEPAUL BUS. & COM. L.J. 439, 442 (2012). As Rice explains,

> The financial services sector falls under a complex web of federal and state regulations designed to govern operations and customer information protection. At the

Regulatory and Interest Rate Control Act in March of 1979.[115] The agencies represented by the council are the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB).[116]

In 1999, The FFIEC implemented section 501(b) of the Gramm-Leach-Bliley Act. This section required FFIEC member agencies to:

> establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[117]

In response to this general call for action, the FFIEC developed security standards similar to those provided in HIPAA. The FFIEC "IT Examination

---

> highest level, the Board of Governors of the Federal Reserve System sets the overall monetary policy for the United States. The activities of a financial services company determine which regulatory body provides oversight. A bank will often fall under several regulatory programs based on the bank's charter and services it offers. Different federal agencies regulate banks offering traditional checking and savings accounts depending on the nature of the bank's charter. Nationally chartered banks fall under the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller for Currency (OCC). Credit unions and state chartered banks fall under the review National Credit Union Administration (NCUA). The FDIC insures deposits held in traditional personal checking and savings accounts.

*Id.*

[115] *About the FFIEC*, FED. FIN. INSTS. EXAMINATION COUNCIL (Mar. 27, 2014), http://www.ffiec.gov/about.htm.

[116] *Id.*

[117] 15 U.S.C. § 6801 (2012). This section provides in relevant part,

> [i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
> (b) Financial institutions safeguards
> In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title, other than the Bureau of Consumer Financial Protection, shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--
> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

*Id.*

Handbook" details those standards and sets forth a multi-step security process to identify and address security needs within a financial institution based on its resources.[118] Among those are a series of security controls comparable to the administrative, physical, and technical safeguards provided in HIPAA.[119] However, there are a number of key differences from which the health care industry may be able to glean valuable lessons for improving security without impeding access.

One of the key distinctions is in the area of user authentication. In 2001, the FFIEC published a new set of guidelines for the financial services industry titled "Authentication in an Internet Banking Environment."[120] This initial guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing internet-based financial services.[121] Changing law and technology, paired with increasing instances of fraud and identity theft from data breaches, prompted the council to update its authentication guidance in 2005.[122] The guidance reiterated its previous risk assessment framework, but also took an important leap in explaining what type of user authentication protections will be considered sufficient.[123]

The FFIEC determined that single factor authentication was no longer sufficient protection.[124] Single factor authentication is the practice of authenticating the identity of a user using only a username and password.[125] The FFIEC guidelines now require institutions to use a three-factor methodology: something the user knows (e.g., a password), something the user has (e.g., an ATM or debit card), and something the user is (e.g., a biometric feature like a fingerprint or retinal scan).[126] The guidelines require the implementation of at least two of the three to meet

---

[118] FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK: INFORMATION SECURITY (2006), *available at* http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf. The process includes several steps: risk assessment, security strategy development, security controls implementation, security monitoring, and security process monitoring and updating. This detailed security process provides guidance to financial institutions with a clear road for determining what safeguards should be implemented to ensure the security of customer information. However, since it is only designed to evaluate a single entity's unique security needs, a full overview is omitted from this Note.

[119] *Id.* at 4.

[120] FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT, *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[121] *Id.*

[122] *Id*.

[123] *Id.*

[124] Rice, *supra* note 114, at 445.

[125] *Id.*

[126] *Id.* at 445–46.

compliance standards.[127] Further, the multi-factor authentication cannot feature two steps from the same category. [128]

Guidance literature regarding HIPAA authentication standards demonstrates a clear preference for three-factor methodology, but falls short of actually requiring that methodology to be used when accessing ePHI.[129] Multi-factor authentication plays a key role in ePHI security as simple password protection is so easily usurped.[130] The lack of a hard rule requiring multi-factor authentication only makes ePHI a more alluring target for savvy hackers who know that huge stores of valuable health and financial information are just a string of characters away. Thus, as financial institutions apply layered authentication, hospital and insurance networks may make for more vulnerable prey.

The FFIEC also recommends the use of a highly sophisticated authentication system called Public Key Infrastructure (PKI).[131] The FFIEC handbook describes PKI as follows:

> The system is based on public key cryptography in which each user has a key pair-a unique electronic value called a public key and a mathematically related private key. The public key is made available to those who need to verify the user's identity.
>
> The private key is stored on the user's computer or a separate device such as a smart card. When the key pair is created with strong encryption

---

[127] *Id.* at 446.

[128] *Id.* For example, an authentication process which required a user to enter a user name and password and then answer a personal question would not be sufficient protection under these standards.

[129] *Security Standards*, *supra* note 74, at 9. This HHS publication states,

> [i]n general, authentication ensures that a person is in fact who he or she claims to be before being allowed to access EPHI. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:
>
> i. Require something known only to that individuals, such as a password or PIN.
> ii. Require something that the individuals possess, such as a smart car, a token, or a key.
> iii. Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.
>
> Most covered entities use one of the first two methods of authentication. Many small provider offices rely on a password or PIN to authenticate the user. If the authentication credentials entered into an information system math those stored in that system, the user is authenticated. Once Properly Authenticated, the user is granted the authorized access privileges to perform functions and access EPHI. Although the password is the most common way to obtain authentication in an information system and the easiest to establish, covered entities may want to explore other authentication methods.

*Id.*

[130] Matt Honan, *Kill the Password: Why a String of Characters Can't Protect Us Anymore*, WIRED MAG. (Nov. 15, 2012), http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all/.

[131] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *supra* note 118, at 26.

> algorithms and input variables, the probability of deriving the private key from the public key is extremely remote. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclosure. The private key is used to create an electronic identifier called adigital signature that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.
>
> The certificate authority (CA), which may be the financial institution or its service provider, plays a key role by attesting with a digital certificate that a particular public key and the corresponding private key belongs to a specific user or system. It is important when issuing a digital certificate that the registration process for initially verifying the identity of users is adequately controlled. The CA attests to the individual user's identity by signing the digital certificate with its own private key, known as the root key. Each time the user establishes a communication link with the financial institution's systems, a digital signature is transmitted with a digital certificate. These electronic credentials enable the institution to determine that the digital certificate is valid, identify the individual as a user, and confirm that transactions entered into the institution's computer system were performed by that user.[132]

The complexity of the PKI framework is what makes it such a highly effective security measure.[133] The main benefit of PKI is that it allows for the secure access of data on a public network and reliably identifies the user accessing the data.[134] Of course, the implementation of such complex authentication security measures raises one of the fundamental issues of electronic data security: the trade-offs.[135] The reality of increased security is that it almost always comes at the cost of convenience.[136] In the health care context, where time is often of the essence, inconvenience can quickly escalate into a danger to the patient's health.[137] So, the security rules for both financial institutions and health care entities are drafted to allow for some flexibility by requiring each entity to conduct a risk assessment to determine the most reasonable security measures given the entity's risks and

---

[132] *Id.*

[133] *Id.*

[134] CARLISLE ADAMS & STEVE LLOYD, UNDERSTANDING PKI: CONCEPTS, STANDARDS, AND DEPLOYMENT CONSIDERATIONS 11–15 (2003).

[135] Honan, *supra* note 130.

[136] *Id.*

[137] Michael J. Schull at al., *The Effect of Low-Complexity Patients on Emergency Department Wait Times*, 49 ANNALS OF EMERGENCY MED. 257 (2007), *available at* http://www.camconnect.org/member/documents/LowComplexityER.pdf.

resources.[138] This flexibility has been criticized by entities looking for more concrete answers to the ever-present question: what are the expectations?[139]

A perfect example of the necessity of a flexible standard is regulation on encryption measures. Encryption utilizes a fixed algorithm to convert electronic data into an incomprehensible code that can only be broken with the use of a variable known as a "key."[140] The FFIEC recognizes the following three types of encryption: the cryptographic hash, symmetric encryption, and asymmetric encryption.[141]

Cryptographic hash encryption encodes data by reducing the variable length of input data into a fixed length input data.[142] Hashes are placed in the code and used to verify the file and message integrity.[143] A cryptographic hash system also uses hashes to encrypt the password that activates the key to unlock the code.[144] Of course, this is not a perfect system and is susceptible to dictionary (or "brute force") attacks wherein a hacker feeds all possible combinations into the algorithm to deduce the password and decrypt the data.[145]

Symmetric encryption also involves the use of a fixed algorithm and key, but unlike cryptographic hash, symmetric encryption is a two-way encryption in which both the creator and the reader use the same key and algorithm to encrypt and decrypt.[146] Since the key is the same for both the creator and the reader, this system relies on the secrecy of the key.[147] If the key is compromised, a hacker can gain access to the data and wreak the sort of havoc experienced by the Surgeons of Lake County.

Asymmetric encryption, which serves as the basis of PKI authentication, creates two distinct but mathematically related keys for the creator and reader.[148] Just as in PKI, these two keys are called the "public" and "private" keys.[149] The reader key

---

[138] *See generally* 45 C.F.R. 164.308(a)(1) (2013); *See also* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *supra* note 118, at 7.

[139] John Moehrke, *Thoughts on Goal III of the ONC HealthIT Strategic Plan*, HEALTHCARE SECURITY/PRIVACY BLOG (Mar. 31, 2011), http://healthcaresecprivacy.blogspot.com/2011/03/thoughts-on-goal-iii-of-onc-healthit.html.

[140] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *supra* note 118, at 52.

[141] *Id.* at 54.

[142] *Id.*

[143] *Id.* For instance, if hashes are obtained from key operating system binaries when the system is first installed, the hashes can be compared to subsequently obtained hashes to determine whether any binaries were changed. *Id.*

[144] *Id.*

[145] *Id.* To protect against that attack, "salt," or additional bits, are added to the password before encryption. The addition of these bits forces attackers to increase the dictionary to include all possible additional bits, thereby making it more difficult to crack the password. *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

must be recognized by the creator key in order for the data to be converted into a digestible form.[150]

Encryption is not a cure all security solution and can in fact weaken a system's security if used inappropriately.[151] For example, security measures which require the regular scanning of network data (i.e., anti-virus software) can be frustrated by encryption.[152] Thus, viruses embedded in encrypted data can go undetected.[153] Encryption also raises the specter of data becoming unavailable should any irregularities occur in data handling or delivery.[154] This presents a substantial risk in the health care context. If a financial institution is unable to access encrypted data, the user may suffer inconvenience or, at worst, lose some money. If a health care emergency medical provider is unable to access an EHR to discover a drug allergy, that inconvenience could cost a life.

## IV. PROPOSED MODIFICATIONS

Based on this review of current regulations, one of the key distinctions between authentication security regulation in the financial and health care industries is the level of guidance provided to covered entities. HIPAA has provided more vague concepts of what is or is not appropriate, but without a more detailed analytical structure the process of risk analysis quickly devolves into a guessing game with harsh consequences for wrong answers.[155]

The complexities and practical realities of health care information technology cannot serve as a deterrent or excuse for failing to provide clearer security standards. Specifically, the financial sector appears to have a much clearer picture of what the minimum standards, or "ground floor," expectations are for authentication measures. By setting a more sophisticated ground floor of security in healthcare systems, many of the recent attacks on healthcare entities by hackers could have been avoided.

---

[150] *Id.*

[151] *Id.* at 51.

[152] *Id.*

[153] *Id.*.

[154] *Id.*

[155] *See* 78 C.F.R. § 5582 (2013).

> In adopting the HITECH Act's penalty scheme, the Department recognized that section 13410(d) contained apparently inconsistent language (i.e., its reference to two penalty tiers "for each violation," each of which provided a penalty amount "for all such violations" of an identical requirement or prohibition in a calendar year). To resolve this inconsistency, with the exception of violations due to willful neglect that are not timely corrected, the IFR adopted a range of penalty amounts between the minimum given in one tier and the maximum given in the second tier for each violation and adopted the amount of $1.5 million as the limit for all violations of an identical provision of the HIPAA rules in a calendar year. For violations due to willful neglect that are not timely corrected, the IFR adopted the penalty amount of $50,000 as the minimum for each violation and $1.5 million for all such violations of an identical requirement or prohibition in a calendar year.

*Id.*

Perhaps just as important, clearer standards would allow the Office of Civil Rights to more effectively enforce those standards.[156]

The question then necessarily becomes, "what should be the ground floor?" The most direct way to address this problem is to raise the baseline security standards for encryption and authentication security. These new encryption and authentication security standards must be set forth in a way that is consistent with the flexible framework that currently pervades HIPAA. This will necessarily require a balancing between providing strict standards and allowing covered entities adequate discretion to implement those standards in a manner that suits their needs and resources.

The first proposed amendment is changing encryption of ePHI from an "addressable" measure to a "required" measure. Covered entities who utilize networked devices, that is, devices that are capable of transmitting ePHI over the internet, would be required to encrypt that data to ensure the data cannot be viewed by a hacker who gains remote access to the server. This is the most effective security framework available and is consistent with the other major proposed amendment that requires three-step authentication.

Some covered entities may argue that an encryption requirement is overly burdensome. This is in part a concern about the strain encryption can place on a computer's processing speed. While this may be a concern for older computers, modern technology is trending toward more efficient processing that makes encryption more affordable.[157] Further, HHS already recommends encryption utilization as a way to ensure compliance with security requirements.[158] HHS also notes that smaller to mid-size practices are specifically being targeted by hackers because they tend to adopt only the bare minimum of security requirements.[159] By making encryption an essential part of all EHR software, hackers will have to look elsewhere to gain easy access to sensitive personal information. When encryption is already the industry norm, and technology is moving to support EHR encryption, there appears little chance of a technological retreat in encryption technology. The most logical step is to establish encryption as a basic element of EHR security by requiring all covered entities to utilize it.

The second proposed amendment is to "require" three-step authentication to access ePHI. HHS has already "strongly encouraged" three-step authentication to protect HER, and three-step authentication is required in the financial industry.[160] Three-step authentication also utilizes a PKI framework that has proven to be the most effective at preventing unauthorized intrusions.

---

[156] Rachel Grunberger, *Senate Hearings Focus on Lack of HIPAA Enforcement, Final HITECH Rule*, INSIDE PRIVACY BLOG (Dec. 22, 2011), http://www.insideprivacy.com/senate-hearings-focus-on-lack-of-hipaa-enforcement-final-hitech-rule/.

[157] *Encrypt Data with Performance Using Intel® Xeon® Processors*, INTEL CORP. (2012), http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/encrypt-healthcare-data-with-performance-using-intel-xeon-processors.pdf. This article highlights how technology can improve CPU efficiency to support encryption with Epic software. Epic is the most popular EHR software on the market today.

[158] HEALTHIT.GOV, *supra* note 53, at 13.

[159] *Id.*

[160] SECUREIT, UNDERSTANDING THE SECURITY AND PRIVACY RULES UNDER THE HIPAA AND HITECH ACTS 11 (2011), www.secureit.com/resources/WP_HIPAA_HITECH_CMS_final_072811.pdf.

At first glance, requiring three-step authentication may seem inconsistent with the flexible standards throughout HIPAA. Three-step authentication is a more strict requirement than merely any "reasonable and appropriate measure," but it still allows for considerable discretion in determining the level of sophistication a covered entity could implement. As outlined in the previous section, current banking regulations allow financial institutions to choose from two of three general means of authentication: (1) something the user knows, (2) something the user has, and (3) something the user "is." By leaving it up to the covered entity to decide which two means to implement, the costs and burdens associated with a three-step authentication system become very flexible. For example, a large covered entity with huge stores of ePHI and sophisticated resources could require both a password and biometric authentication, such as fingerprint or retinal scans, to access its network. A smaller practice can opt for the much simpler and cost-effective password and key card combination.

With any increased security standard there is a legitimate concern that healthcare providers will be forced to divert valuable time and monetary resources away from patient care and into compliance efforts. But increased security standards do not necessarily distract providers from their primary role as caregivers. In fact, third-party EHR vendors, not providers, will bear most of the burden of these proposed changes. A recent survey by Software Advice, a group which conducts consumer research on software products, revealed that just five EHR software vendors enjoy an eighty-five percent market share among outpatient physicians who utilize EHR technology.[161] The largest provider, Epic, provided roughly twenty percent of outpatient EHR software.[162] The Epic website states that 760,000 patient records are exchanged each month on its servers.[163] Given this concentration of market share, compliance with the regulations will primarily fall on these few major EHR vendors who specialize in information technology security and are in the best position to implement the new requirements across the industry.

Finally, if quality patient care is the ultimate goal of healthcare, then the costs associated with raising security standards for encryption and authentication under HIPAA are outweighed by the increase in consumer trust that will follow implementation. As noted earlier, there is still considerable skepticism among patients about the overall security of EHR technology.[164] That skepticism can have a negative impact on the trust relationship between a provider and patient. The level of trust a patient has in his or her provider has been linked to the overall quality of care.[165] Bringing HIPAA security standards into the twenty-first century demonstrates to healthcare consumers that their ePHI security is taken seriously and that EHR technology should be a source of promise, not fear.

---

[161] *EHR Market Share Analysis*, HEALTHCARE IT NEWS (May 20, 2010), http://www.ehrwatch.com/headline/ehr-software-market-share-analysis.

[162] *Id*.

[163] *See About Us*, EPIC SYS. CORP., http://www.epic.com/about-index.php (last visited Aug. 27, 2014).

[164] Love, s*upra* note 22, at 15.

[165] Kao et al., s*upra* note 25.

Given the above analysis, the following are proposed modifications to current HIPAA technical safeguards provided in 45 C.F.R. § 164.312. These new minimum standards can achieve needed security minimums without overly burdening EHR developers or the health care providers, and patients who utilize EHRs.

45 C.F.R. § XXXX

§ XXXX Definitions

As used in this part, the following terms have the following meanings:

(a) Authentication: A system, technology, or process that ensures the integrity, security, and authenticity of electronic transactions of Protected Health Information conducted via an unsecured, public network.

(b) Protected Health Information: includes individually identifiable health information

(1) That is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

(c) Electronic Protected Health Information: means information that comes within (1)(i), (1) (ii), or (1)(iii) of this section.

(d) Transaction: means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

(e) Implementation specification: means specific requirements or instructions for implementing a standard.

§ 164.312 Technical Safeguards.

A covered entity must:

(a)

(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Required). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Required). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)

(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) Implementation specification: Mechanism to authenticate electronic protected health information (Required). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(1) Implementation specification: Authentication must utilize a three-factor methodology, that includes at least two of the following:

(i) Something the user knows (i.e., a password)

(ii) Something the user has (i.e., a magnetic identification card)

(iii) Something the is (i.e., a biometric feature such a retinal scan or fingerprint)

(2) Implementation Specification Public Key Infrastructure Authentication (addressable): PKI authentication is the preferred means for authenticating the transmission of all electronic Protected Health Information over a non-secure network. PKI should consist of:

(i) A certificate of authority (CA) that both issues and verifies the digital certificates;

(ii) A registration authority which verifies the identity of users requesting information from the CA;

(iii) A central directory—i.e. a secure location in which to store and index keys;

(iv) A certificate management system; and

(v) A certificate policy.

(e)

(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network consistent with § 164.312(d)(2).

(2) Implementation specifications:

(i) Integrity controls (Required). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Required). Implement a mechanism to encrypt electronic protected health information whenever electronic protected health information is transmitted via a public non-secure network.

(iii) Assymetric encryption (Addressable): mathematically related but distinct public keys and private keys should be used for encryption of electronic protected health information, in accordance with § 164.312(d)(2) and otherwise whenever appropriate.

## V. CONCLUSION

Mobile technology and remote access to ePHI are now the norm in the medical field. The many advantages of remote access, such as convenience and improved integration of care, are counterbalanced by increased risk that unauthorized users will gain access to that information. While heightened regulation cannot stop all intrusions into ePHI, it can make it harder for hackers to gain access to patient information by raising the baseline standard for security across the industry. While current legislation encourages the adoption of some basic security measures, such as encryption and multi-layer authentication, it fails to make them outright requirements.

If the healthcare industry is going to move into the twenty-first century, and realize the dramatic potential of widespread EHR adoption, it must first catch up to the security norms that prevail in the modern technological landscape. The industry cannot afford to ease into security by allowing covered entities to utilize outdated and ineffective security measures until they self-determine that it is reasonable and appropriate to adopt security technology that is already the norm in a comparable industry.

The changes proposed in this Note are already basic requirements in the financial sector where personal financial information is regularly transmitted. These changes would implement the same basic level of security across the healthcare industry, while still recognizing the need for individual discretion among covered entities in determining what measures best fit their needs and budget. These heightened security standards would not only bring the healthcare industry in line with the comparable financial industry, but would help improve consumer confidence in providers that utilize this valuable technology.