2017

Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals

Deborah R. Farringer
Belmont University - College of Law

Recommended Citation
40 Seattle U. L. Rev. 937 (2017)

Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals

Deborah R. Farringer[*]

CONTENTS

INTRODUCTION

On the morning of March 28, 2016, several employees of MedStar Health ("MedStar"), a nonprofit hospital system with ten hospitals in

[*] Deborah R. Farringer is an Assistant Professor of Law at Belmont University College of Law in Nashville, TN. J.D., Vanderbilt University Law School; B.A., University of San Diego. I would like to thank my research assistants Kim Macdonald and Grace Ann Miller for their work and help in bringing this article to fruition. Thanks also to Carinne Jaeger, Megan Livres, and all of the editorial staff of Seattle University Law Review for their very helpful suggestions and edits to this article. Finally, thank you to my husband and children for their patience with me through this process.

Maryland and Washington, D.C.[1] were greeted with a pop-up message stating: "You just have 10 days to send us the Bitcoin . . . [A]fter 10 days we will remove your private key and it's impossible to recover your files."[2] The demand was 45 bitcoin,[3] which is equivalent to approximately $19,000.[4] If the hospital paid the bitcoin ransom, the hackers claimed they would provide the necessary information to enable MedStar to regain access to its system.[5] Consistent with recommendations from federal officials, it appears that MedStar chose not to pay the bitcoin ransom.[6] Without its electronic health records ("EHR") system, MedStar was forced to shut down its email and computers for all of its ten hospitals and its approximately 250 outpatient centers.[7] The ramifications went beyond simply shutting down email and computers, however. While the

1. *Our Locations*, MEDSTAR HEALTH (May 18, 2016), http://www.medstarhealth.org/mhs/our-locations/#q={}[https://perma.cc/RBG3-9HXL].

2. John Woodrow Cox, *MedStar Health Turns Away Patients After Likely Ransomware Cyberattack*, WASH. POST (Mar. 29, 2016), https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html [https://perma.cc/9GY8-H3YX] (citing to note appearing on computer screens of employees sent by malware hackers).

3. *Id.*

4. Bitcoin is an online currency created in 2009, by an individual referred to as Satoshi Nakamoto, which is thought to be an alias. *See* Tal Yellin, et al., *What is a Bitcoin*, CNN MONEY, http://money.cnn.com/infographic/technology/what-is-bitcoin/ [https://perma.cc/8C3M-U4LM]; *see also* Chad Bray, *Australian Ends Attempt to Prove He Founded Bitcoin*, N.Y. TIMES: DEALBOOK (May 5, 2016), http://www.nytimes.com/2016/05/06/business/dealbook/australian-ends-attempt-to-prove-he-founded-bitcoin.html?_r=0 (reporting that the mystery of the inventor of Bitcoin remains after Craig Steven Wright admitted that he was not, in fact, the inventor, contrary to his own previous assertions and articles in *Wired* and *Gizmodo* in 2015 that identified Wright as Nakamoto). The intention behind the currency is that the transacting parties can exchange the currency directly without a bank or any other third party transacting agent (as would be the case with credit cards, which often have associated credit card fees). Yellin, *supra*. Bitcoins can be purchased on a bitcoin exchange, which allows individuals to either buy or sell bitcoin using various currencies (dollars, euros, pounds, etc.). *Id.* One of the features of a bitcoin exchange is that the names of the individual buyers and sellers are not revealed. Rather, the transaction is logged as being between wallet IDs. *Id.* This anonymity makes it difficult to ever trace the wallet ID back to the buyer or seller, and thus, Bitcoin has become a popular vehicle for purchasing drugs or other illicit activities online. *Id.*

5. Cox, *supra* note 2.

6. *See* Rachael King, *FBI Cyber Division Chief Advises Companies Not to Pay Ransom for Release of Data*, WALL ST. J.: CIO J. (May 4, 2016, 1:24 PM), http://blogs.wsj.com/cio/2016/05/04/fbi-cyber-division-chief-advises-companies-not-to-pay-ransom-for-release-of-data/ [https://perma.cc/25MY-L4XX]. *See* Mark Hagland, *The Cyberattack on the 10-Hospital MedStar Health Poses Several Important Questions to Patient Care Leaders*, HEALTHCARE INFORMATICS (Apr. 4, 2016), http://www.healthcare-informatics.com/blogs/mark-hagland/so-it-was-ransomware-implications-attack-medstar-health [https://perma.cc/NDM8-3F2Z] ("A bitcoin tracking site reports that no funds have been transferred in or out of [the online 'wallet' that MedStar was directed to in order to pay the ransom demand].").

7. Cox, *supra* note 2.

emergency department in MedStar's Washington, D.C. hospital stayed open during the outage, the challenges with triaging and treating patients utilizing a back-up paper system eventually led to diversion of patients with life-threatening conditions to other area hospitals.[8] Moreover, many of MedStar's outpatient clinics were forced to cancel appointments entirely, as some were unable to provide treatment or other routine office management functions, such as check-in, billing, and collection, without their computer system in operation.[9] Beyond the inconveniences of slow response time and rescheduling of certain outpatient appointments, lack of access to the EHR system created patient care concerns and potential safety risks.[10] For example, a nurse reported to *The Washington Post* that, because of delayed lab results, she continued to give certain medication—"with a number of potentially serious side effects"—to a patient whose medication should have been discontinued eight hours earlier.[11] While MedStar executives tried to remain positive to the public, the narratives from patients, providers, and staff about the challenges presented with this sort of attack revealed a different story.[12]

While a malware attack like this may be a mere annoyance or inconvenience for some businesses, the challenges presented to healthcare providers in this context can be much more devastating.[13] Unfortunately, stories like that of MedStar are not isolated. Within weeks of the MedStar attack, there were reports of attacks on one hospital in Kentucky, two

---

8. *Id.*

9. *Id.*

10. *Id.* (noting that a man receiving cancer treatment was unable to receive radiation treatment for two days because of the shutdown).

11. *Id.*

12. *Id.* ("Without access to email and computer systems, the medical staff fell back on seldom-used paper records . . . [which] are far less comprehensive than those kept in digital form. They can be missing vital pieces of patient information . . . ."). *See also* Jürgen Stausberg, et al., *Comparing Paper-based with Electronic Paper Records: Lessons Learned during a Study on Diagnosis and Procedure Codes*, 10 J. AM. MED. INFORMATICS ASS'N 470 (Sept./Oct. 2003), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC212784/ [https://perma.cc/MT7J-6D6T] (noting that often times the electronic record contains distinct data and finding that "parallel use of electronic and paper-based patient records result[ed] in inconsistencies between the record systems' and 'documentation [was] missing in both.").

13. *See* Naomi Lachance, *Malware Attacks on Hospitals Put Patients At Risk*, NASHVILLE PUB. RADIO (Apr. 1, 2016), http://www.npr.org/sections/alltechconsidered/2016/04/01/472693703/malware-attacks-on-hospitals-put-patients-at-risk [https://perma.cc/42YJ-VJNR] (quoting Kevin Fu, Associate Professor at the University of Michigan, "[t]he big difference with health care is that the consequences are greater . . . . You can lose your email and that's annoying, but patient records are needed in order to treat patients."); Nsikan Akpan, *Has Health Care Hacking Become an Epidemic?*, PBS NEWSHOUR (Mar. 23, 2016, 6:19 PM), http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/ [https://perma.cc/3PK6-W9M3] (noting that there are fewer protections for health data, but such data is also more valuable because of the amount of information that is contained in such records).

hospitals in California, one hospital in Kansas, and one hospital in Ottawa, Canada.[14] Hollywood Presbyterian Medical Center in Los Angeles, California announced that it had paid the 40 bitcoin ransom demand (equivalent to about $17,000) in order to regain access to its system.[15] Kansas Heart Hospital, in Wichita, also paid a bitcoin ransom in an effort to regain access to its EHR system, but it gained only "partial access" and a demand for additional money.[16] While hackers and data breaches are not new in the healthcare context,[17] ransomware attacks[18] are unique in the way they have a direct and immediate impact on the actual provision of care to patients and present a very real threat to patient safety.[19] Sadly, the potential devastation that could be caused when hospitals and health systems lose access to their EHRs and computer systems[20] is exactly what makes these types of attacks so attractive to potential hackers.[21] As these attacks are starting to become more commonplace, many are questioning how the healthcare industry has become so vulnerable and what can be

14. Marianne Kolbasuk McGee, *Ransomware: Time for a HIPAA Update?*, INFORISK TODAY (Mar. 29, 2016), http://www.inforisktoday.com/ransomware-time-for-hipaa-a-9002 [https://perma.cc/48KQ-RH8Z].

15. *Id.*; Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016, 10:44 AM), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html [https://perma.cc/HD2M-QUSH].

16. Justin Pot, *Ransomware Attackers Refuse to Decrypt Hospital's Files After Being Paid Off*, DIGITAL TRENDS (May 24, 2016, 4:43 PM), http://www.digitaltrends.com/computing/ransomware-hospital-hackers-demand-more-money/ [https://perma.cc/GL82-N9BC].

17. *See* Claire Groden, *This Big U.S. Health Insurer Just Got Hacked*, FORTUNE (Sept. 10, 2015), http://fortune.com/2015/09/10/hack-health-insurer-bluecross/ [https://perma.cc/73J8-TZZ2] (noting that Excellus BlueCross BlueShield announced that more than ten million of its customers' information—including social security numbers, names, addresses, birthdates, financial information, and claims—had been exposed in a cyberattack); Kara Scannell & Gina Chon, *Cyber Security: Attack of the Health Hackers*, FIN. TIMES (Dec. 21, 2015), http://www.ft.com/cms/s/2/f3cbda3e-a027-11e5-8613-08e211ea5317.html#axzz49JER10mJ [https://perma.cc/7ZBE-PQ5Q] (reporting that hackers believed to be from China used administrator's credentials to access health insurer Anthem's database to access personal information such as names, social security numbers, and birthdates of over seventy-eight million people).

18. Ransomware is a type of malware that blocks users from accessing their data until a ransom is paid. *See* Zetter II, *infra* note 105.

19. Unlike cyberattacks intended to access personal data, a cyberattack that prevents access to an EHR disrupts the ability of a provider to actually provide care in the same manner. Erin McCann, *Nurses Want Probe into EMR Failure*, HEALTHCAREIT NEWS (Mar. 10, 2015, 11:23 AM), http://www.healthcareitnews.com/news/rns-want-investigation-emr-failure [https://perma.cc/6FSM-FH2E] (noting all of the issues that arose at Antelope Valley Hospital in Lancaster, California when its EHR crashed).

20. When referring to an EHR, this Article considers not only the records themselves, but the "front end" and "back end" system components that permit a provider to schedule patients and also bill and process claims for services already provided.

21. Andrea Peterson, *Why Hackers Are Going After Health-Care Providers*, WASH. POST: THE SWITCH (Mar. 28, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/why-hackers-are-going-after-health-care-providers/ [https://perma.cc/6V6H-4MZX].

done to stop the cycle of attacks.[22] Despite efforts by the United States Congress to increase reporting of cyberattacks[23] and efforts by the Department of Commerce to increase education and awareness on cybersecurity,[24] more needs to be done in order to prevent these attacks and provide greater protection not just of patient data but also of the EHRs and computer systems upon which patients' lives depend.

Hospitals and health systems appear uniquely vulnerable to ransomware attacks as a result of various factors, including (1) the fractured movement toward electronic medical records and (2) the Department of Health and Human Services' lack of emphasis on enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[25] and the Health Information Technology for Economic and Clinical Health (HITECH) Act[26] with respect to security of electronic data. This Article argues that, while stricter and more current federal regulations are necessary, the most expedient way to protect against immediate attacks will be an industry-driven response demanding industry-wide security standards from EHR companies above and beyond HIPAA standards. To accomplish such a response, the healthcare industry will first have to shift from its current electronic security culture that contemplates only the minimum necessary for HIPAA compliance and instead push providers to realize that security of EHRs and patient data will require time, money, and resources in the same way that providers have invested in the latest medical equipment, upgraded facilities, and hired innovative and dynamic personnel in order to compete with one another. Ideally, this shift will also spur a decrease or consolidation of EHR products and offerings—especially those products for specific medical specialties and thus, limited in marketability—into only a few products that will provide more collaboration, system integration, and compatibility among systems. Such consolidation will actually drive

---

22. *Id.*; Akpan, *supra* note 13; *see also* DANIEL W. BERGER, REDSPIN'S BREACH REPORT 2015: PROTECTED HEALTH INFORMATION (PHI) 4 (Feb. 2016) (noting that 98.1% of all "records breached in 2015 were the result of hacking attacks/IT incidents" and that there was an 897% increase in breached records from 2014 to 2015).

23. Cybersecurity Information Sharing Act, 6 U.S.C. §§ 1501–1510 (2015).

24. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., OFF. FOR CIVIL RIGHTS, HIPAA SECURITY RULE CROSSWALK TO NIST CYBERSECURITY FRAMEWORK, (Feb. 2016), http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf [https://perma.cc/FBU8-LJNJ] [hereinafter CROSSWALK].

25. 42 U.S.C. §§ 300gg (2010), 1320d (2010); 29 U.S.C. §§ 1181 (2011), 1182 (2008), 1183 (1996).

26. 42 U.S.C. §§ 300jj to jj-51 (2016), §§ 17901–17903 (2009); Title XIII (Health Information Technology for Economic and Clinical Health Act, "HITECH") of the American Recovery and Reinvestment Act of 2009 (AARA), Pub. L. No. 111-5, 123 Stat. 115, 226-79 (2009) (codified in scattered sections of 42 U.S.C.).

providers closer to the goals envisioned under HIPAA and make security of those systems easier and more reliable.

Part I of this Article describes how the healthcare industry has arrived in this place of vulnerability, including (1) the history of the movement toward EHRs through HIPAA, (2) HIPAA's meaningful use regulations and the background of current ransomware attacks, and (3) the distinctions between these attacks and other security breaches that have plagued large insurers and health systems within the last five years. Next, Part II will examine current industry culture when it comes to cybersecurity and review current legal and business approaches to address this growing threat. Then, Part III will argue that, while the current laws—including HIPAA and HITECH—are a good start, they do not go far enough to curb the current ransomware attacks and thus, should be amended. It will further argue that such amendments cannot be the only solution. Rather, the healthcare industry has to spur its own movement toward better and tighter security over its healthcare technology. Lastly, this Article will conclude with some suggestions and recommendations for how industry and government regulators can work together to assure that hospitals and health systems are not faced with the dilemma of having to choose between patient safety and the payment of a bitcoin ransom.

I. BACKGROUND

A. Origins of HIPAA and the Emergence of Electronic Medical Records

When HIPAA was first enacted in 1996,[27] its objectives were two-fold: (1) assure that individuals could maintain health insurance between jobs; and (2) protect the privacy and confidentiality of patient data as the healthcare industry moved toward electronic transmission of patient data.[28] Although HIPAA was first enacted in 1996, it was not until 2003 that the Department of Health and Human Services (HHS) first enacted regulations addressing privacy (known as the "Privacy Rule")[29] and security of protected health information (known as the "Security Rule").[30] Though HIPAA was intended to move providers toward utilization of

27. Health Insurance Portability and Accountability Act of 1996, H.R. 3103, 104th Cong. (1996) (enacted).

28. *Id.* Note that the first goal of HIPAA was implemented relatively easily, creating the COBRA program that enables individuals to maintain coverage for a period of eighteen months following termination of any job. *See* BARRY R. FURROW ET AL., HEALTH LAW CASES, MATERIALS AND PROBLEMS 750–51 (7th ed. 2013).

29. The Privacy Rule and Security Rule are combined in the HIPAA Administrative Simplification Regulations. *See* 45 C.F.R. §§ 160 (2014), 162 (2011), 164 (2013).

30. *Id.*

EHRs,[31] at first the law did little to actually change the practices of many providers to move away from paper records systems.[32] As Dr. David Blumenthal of the U.S. Office of the National Coordinator for Health Information Technology (ONC) noted in 2010: "We have years of professional agreement and bipartisan consensus regarding the potential value of EHRs. Yet we have not moved significantly to extend the availability of EHRs from a few large institutions to the smaller clinics and practices where most Americans receive their health care."[33] Indeed, a report from the ONC found that, by 2008, only 9.4% of hospitals had a basic EHR system.[34] While widely believed to help mend some of the fragmentation of the current U.S. healthcare system and provide better patient outcomes through enhanced communication and care coordination, hospitals and other practitioners were slow to adopt new technology.[35]

Even acknowledging the benefits, implementation of an EHR system requires capital investment in new equipment and software, training time for staff, redesigning of clinical processes and workflow, disruption of billing and collection, and new compliance requirements.[36] Thus, implementation of an EHR system is neither an easy nor inexpensive proposition for providers.[37] While providers may adjust over time, it has been reported that EHRs "can potentially decrease individual provider

---

31. Following the enactment of HIPAA, the George W. Bush Administration began pushing healthcare providers toward a national EHR, stating in 2004 that it had a ten-year goal that the U.S. implement a national EHR by 2014. *See* Nicolas P. Terry, *Certification and Meaningful Use: Reframing Adoption of Electronic Health Records as a Quality Imperative*, 8 IND. HEALTH L. REV. 43, 48 (2011) (citing White House Off. of the Press Sec'y, *Fact Sheet: Transforming Health Care for All Americans* (May 27, 2004), http://georgewbush-whitehouse.archives.gov/news/releases/2004/05/20040527-2.html).

32. JAWANNA HENRY ET AL., ADOPTION OF ELECTRONIC HEALTH RECORD SYSTEMS AMONG U.S. NON-FEDERAL ACUTE CARE HOSPITALS: 2008-2015, 35 ONC DATA BRIEF 1, (May 2016), https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php [https://perma.cc/ZA52-QTNE].

33. David Blumenthal & Marilyn Tavenner, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 NEW ENG. J. MED. 501, 501 (2010).

34. HENRY ET AL., *supra* note 32.

35. *Id.*; Nir Menachemi & Taleah H. Collum, *Benefits and Drawbacks of Electronic Health Record Systems*, RISK MGMT. & HEALTHCARE POL'Y 47 (May 11, 2011), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3270933/pdf/rmhp-4-047.pdf [https://perma.cc/68WG-LTM9] (noting that electronic health records have the ability to revolutionize the healthcare industry, but noting the functional, financial, productivity, and privacy and security concerns).

36. Agency for Healthcare Res. & Quality, *Electronic Medical Record Systems*, HEALTH INFO. TECH., https://healthit.ahrq.gov/key-topics/electronic-medical-record-systems [https://perma.cc/S2BJ-XTBM] (citing various barriers to adoption of an EHR, including "[h]igh capital cost and insufficient return on investment for small practices and safety net providers[, u]nderestimation of the organizational capabilities and change management required[, and f]ailure to redesign clinical process and workflow to incorporate the technology systems").

37. *See id.*; *see also* Menachemi & Collum, *supra* note 35, at 51.

productivity by 10%" and can add additional costs for maintenance of the system as well as storage of the data on a long-term basis.[38] Knowing that spurring providers (especially smaller providers) into implementing an EHR would be a challenge, HHS tried other incentives prior to enactment of HITECH to push providers toward use of electronic records.[39] HHS created a safe harbor under the federal Anti-kickback Statute and an exception to the Physician Self-Referral Law (otherwise known as the Stark Law) that would permit hospitals to provide certain hardware and software to referring physicians to adopt an EHR system or to enable physician practices to have e-prescribing capabilities.[40] Additional funding was given to states for the establishment of regional health information exchanges (RHIOs),[41] designed to encourage providers in a particular region to share medical information in a central location (or "vault") enabling other providers to access the data as patients seek care from various providers in the region.[42] Since enactment of HITECH, there have been additional (albeit distinct) efforts[43] toward other medical

38. Dean F. Sittig & Hardeep Singh, *Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use*, 127 PEDIATRICS e1042, e1045 (Apr. 2011), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3065078/ [https://perma.cc/3ART-QXJU] (noting further that many providers are concerned about cost, given the ongoing expense, offset by the fact that an estimated 89% of the monetary benefits of an EHR actually inures to health insurers (or payors)).

39. *Id.*

40. *See* 42 C.F.R. § 1001.952(x), (y) (2017); 42 C.F.R. § 411.357(v), (w) (2017).

41. The primary goals of RHIOs are to enable better patient care through a reduction in overtreatment and duplicative care enabled through access to information among providers. Julia Adler-Milstein et al., *The State of Regional Health Information Organizations: Current Activities and Financing*, 27 HEALTH AFFS. 60, 61 (2007), http://content.healthaffairs.org/content/27/1/w60.full.pdf+html [https://perma.cc/J5KA-97BM].

42. 42 U.S.C. § 300jj-31(a)(1) (2009) (directing the Secretary of HHS to invest in infrastructure necessary to support "health information technology architecture that will support the nationwide electronic exchange and use of health information in a secure, private, and accurate manner, including connecting health information exchanges "); *see also* 42 U.S.C. § 300jj-31(a)(2)–(7) (2009) (HITECH also provided funding for the Secretary of HHS to support "(2) [d]evelopment and adoption of appropriate certified electronic health records for categories of health care providers not eligible for support under title XVIII or XIX of the Social Security Act . . . for the adoption of such records[;] (3) [t]raining on and dissemination of information on best practices to integrate health information technology, including electronic health records, into a provider's delivery of care . . . [;] (4) [i]nfrastructure and tools for the promotion of telemedicine . . . [;] (6) [p]romotion of technologies and best practices that enhance the protection of health information by all holders of individually identifiable health information [; and] (7) [i]mprovement and expansion of the use of health information technology by public health departments.").

43. Despite some initial excitement around RHIOs, the majority of the projects have been largely abandoned due to a variety of factors, including complex and detailed regulations and movement toward other collaboration and consolidation efforts. *See* Joshua M. Liao & Danny Chu, *The State of Health Information Exchange*, 3 J. HEALTH MED. INFO. 1 (2012), http://www.omicsonline.org/the-state-of-health-information-exchange-2157-7420.1000e102.pdf [https://perma.cc/9BL9-M8JC].

records integration. The most impactful effort is perhaps the creation of accountable care organizations (ACOs) under the Affordable Care Act (ACA), which requires clinical integration that can be accomplished through coordination and/or consolidation of EHRs.[44] None of the efforts, however, have been able to fulfill HIPAA's stated goals regarding better communication among providers. Rather, to date, the principal effort has been simply moving providers toward adoption of *any* electronic records system.[45]

It was this slow response by providers and seemingly stagnant approach to EHR adoption that spurred enactment of the HITECH Act in 2009.[46] HITECH's "meaningful use" standards directed hospitals and other health care providers not only to possess a "certified EHR" system[47] but also to "meaningfully use" health information technology.[48] Demonstration of "meaningful use" under the regulations requires the provider to meet "certain measurement thresholds that range from recording patient information as structured data to exchanging summary care records."[49] These measurements are established in three different stages.[50] In an effort to assure compliance, HHS utilized funding appropriated by Congress to enact regulations to encourage and promote

---

44. Patient Protection and Affordable Care Act, 42 U.S.C. § 1395jjj (2016); *see also* Statement of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program, 76 Fed. Reg. 67026, 67027 (Oct. 28, 2011).

45. The first set of regulations for Stage 1 was published in 2010. *See* 75 Fed. Reg. 44,314 (July 28, 2010).The Centers for Medicare and Medicaid Services (CMS) has subsequently issued regulations for Stage 2. *See* 77 Fed. Reg. 53,968 (Sept. 4, 2012). For Stage 3, see 80 Fed. Reg. 16,732 (Mar. 30, 2015).

46. 42 U.S.C. §§ 300jj to jj-51 (2016).

47. The ONC has officially removed the definition of certified EHR technology from its definitions, but generally defines it as an EHR that supports the EHR Incentive Programs, as set forth in the EHR Incentive Programs regulations. *See* Off. of the Nat'l Coordinator for Health Info. Tech., *Certified EHR Technology Definition*, HEALTHIT.GOV, https://www.healthit.gov/policy-researchers-implementers/certified-ehr-technology-definition [https://perma.cc/D3KY-VEMB].

48. 42 U.S.C. §§ 300jj to jj-51.

49. Office of the Nat'l Coordinator for Health Info. Tech., *Meaningful Use Regulations*, HEALTHIT.GOV, https://www.healthit.gov/policy-researchers-implementers/meaningful-use- regulations [https://perma.cc/Z33K-E9NB].

50. *Id.* One of the primary goals of the meaningful use requirements was to assure that not only did providers purchase an EHR but also that they purchase one that is more than simply an electronic filing system in which all paper records are simply stored online in PDF format. This is evident from the various stages of the meaningful use regulations. Once providers adopted an EHR under Stage 1, they move to Stage 2, which "encouraged the use of health IT for continuous quality improvement at the point of care *and the exchange of information in the most structured format possible*." Ctrs. for Medicare & Medicaid Servs., *Electronic Health Records (EHR) Incentive Programs*, CMS.GOV, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms [https://perma.cc/8SGP-C8H6] (emphasis added).

adoption of EHRs through a "carrot and stick" approach.[51] In doing so, HHS initially encouraged adoption and use of EHRs through financial incentives to providers[52] but, after four years, began assessing penalties for any providers who failed to adopt and use EHRs.[53]

The incentives and penalties seem to have accomplished at least some of HITECH's intended goals. By 2015, 96% of all non-federal acute care hospitals possessed a certified EHR system, with 84% of those hospitals adopting a basic EHR system.[54] While it certainly spurred providers to finally purchase, and in some cases adopt, an EHR system,[55] this rapid ascent into EHR adoption seems to have caused some unintended consequences.[56] As one author has noted,

> Unlike other sectors that implemented IT naturally and gradually over the course of many years, health care went digital overnight, after the government allocated billions of dollars to promote adoption of electronic health care records . . . . This explosive growth rate is alarming and indicates that health care entities could not have the organizational readiness for adopting information technologies over such short period of time.[57]

In addition to challenges with organizational readiness, the almost instantaneous demand for EHRs, without emphasis or requirement in the regulations for any compatibility between systems, has resulted in a lack of interoperability between health information technologies among providers both regionally and across the country.[58] Indeed, initial HITECH

---

51. Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 181 (2014).

52. 42 U.S.C. § 1395w-4(o) (2016).

53. Samantha Burch, *Meaningful Use—Stage 3 Coming, Stages 1 and 2 Compliance*, 20150325 AHLA SEMINAR PAPERS 9 (Mar. 25, 2015); American Recovery and Reinvestment Act, Pub. L. No. 111-5, 123 Stat. 115 (2009); 42 U.S.C. § 1395w-4.

54. HENRY ET AL., *supra* note 32. This information is based on non-federal acute care hospitals. A basic EHR system is defined as a system that has a "minimum use of 10 core functionalities determined to be essential to an EHR system." *Id.* As noted above, a certified EHR is an EHR that has technology certified to meet federal requirements. The importance of this distinction is that while nearly 97% of hospitals possessed an EHR that meets minimum requirements under federal regulations, only about 76% of hospitals had implemented and were using a basic EHR in 2014. *Id.* The statistics were largely unchanged for reporting year 2015.

55. While many providers purchased an EHR, not all providers actually began using it or adopted its use as contemplated by the meaningful use regulations. *See* Niam Yaraghi, *A Health Hack Wake-Up Call*, U.S. NEWS & WORLD REP. (Apr. 1, 2016, 9:00 AM), http://www.usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call [https://perma.cc/66YG-LD8E].

56. *Id.*

57. *Id.*

58. George Palma, *Electronic Health Records: The Good, The Bad, and the Ugly*, BECKER'S HEALTH IT & CIO REV. (Oct. 14, 2013), http://www.beckershospitalreview.com/healthcare-

regulations focused on providers' *use* of an electronic system in an attempt to transition providers away from paper records and also away from purchasing systems that effectively provided an online electronic record filing system.[59] As Stage 1 focused on getting hospitals to adopt EHRs, later Stages 2 and 3 of the HITECH program shifted to incorporation of some health information exchange (such as orders and tests), greater patient interaction and access to one's own health system, transitions in care, decision support, and improving population health outcomes.[60] Despite the newfound accessibility the EHR provides, few metrics or measurements focus on an ability to communicate health information across various spectrums of care.[61] Although there may be additional goals in the coming years,[62] thus far the regulations have not focused on the coordination of those EHR systems among providers, that is, the ability of various EHR systems to "talk" to one another.[63] Contrary to some of the

---

information-technology/electronic-health-records-the-good-the-bad-and-the-ugly.html [https://perma.cc/RJD6-7E26] (stating that sharing information within networks of referring hospitals is frequently not possible, as may providers are unwilling to open the lines of communication and little planning for integration is being put into place).

59. Electronic Health Record Incentive Program, 75 Fed. Reg. 44,314, 44,321 (July 28, 2010).

60. *Id.*

61. *Id.* at 44321–22. Stage 1 of the program, effective in 2011, was for the purpose of data capture and sharing; Stage 2, effective in 2014, was for the purpose of advancing clinical processes, and Stage 3, effective in 2016, was for the purpose of improved outcomes. *See* Office of the Nat'l Coordinator for Health Info. Tech., *Meaningful Use Definition & Objectives*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives [https://perma.cc/JLE5-JKFR].

62. It should be acknowledged here that part of the reason that RHIOs and other efforts regarding interoperability have remained relatively stagnant is the simultaneous efforts under the Affordable Care Act of 2010 (ACA) to create accountable care organizations (ACOs). *See* Patient Protection and Affordable Care Act, 42 U.S.C. § 1395jjj (2016). ACOs, defined as "groups of doctors and other health care providers who voluntarily work together with Medicare to give high quality service to Medicare Fee-for-Service beneficiaries," contemplate clinical integration in order to meet federal requirements, including requirements set forth by the Federal Trade Commission, regarding these sorts of activities. *See* Dep't of Health & Human Servs., Ctrs. for Medicare & Medicaid Servs., *Shared Savings Program*, CMS.GOV, https://www.cms.gov/Medicare/Medicare-Fee-For-ServicePayment/sharedsavingsprogram/index.html [https://perma.cc/2AWB-GLBE]; State of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program, 76 Fed. Reg. 67,026, 67,027 (Oct. 28, 2011). Because quality metric reporting and clinical integration typically requires sharing of data, one of the goals of ACOs is to create this interoperability or data sharing between providers. Thus, as the provisions of the ACA are now being implemented and ACOs and other initiatives such as value-based purchasing push providers toward integration, many are waiting to see whether interoperability will come about as a result of these other efforts toward integration and payment reform. *See* Joseph Conn, *Interoperability Hurdles Impede ACOs*, MOD. HEALTHCARE (Jan. 20, 2016), http://www.modernhealthcare.com/article/20160120/NEWS/160129991 [https://perma.cc/4RAG-TSRB].

63. U.S. GOV'T ACCOUNTABILITY OFF., GAD-15-817, ELECTRONIC HEALTH RECORDS: NONFEDERAL EFFORTS TO HELP ACHIEVE HEALTH INFORMATION INTEROPERABILITY, http://www.gao.gov/assets/680/672585.pdf [https://perma.cc/F67Y-8MZG] (noting five key

initial intentions of HIPAA to utilize EHRs for the purpose of sharing data among providers across the continuum of care, the focus under HITECH seems to be driven by the goals of compliance and reporting.[64]

Just as the regulations have not focused on interoperability, there has been little emphasis on a need to update, revise, or reevaluate the security regulations drafted under HIPAA.[65] Even with enactment of HITECH, there have been no updates or amendments to the security regulations issued under HIPAA since it was finalized in 2003.[66] Many critics feel that the security provisions are already many years out of date and, as a consequence, do little to actually protect data as necessary to account for the current state of cybersecurity.[67] CynergisTek, Inc.[68] co-founder and CEO Mac McMillan has stated,

> We're behind . . . [b]asically what we really need to do is scrap the HIPAA Security Rule and just let organizations select the framework that they want to work with, whether it's [National Institute of Standards and Technology (NIST)], whether it's [International Organization for Standardization (ISO)], but a legitimate framework. From there, they build their program and we hold them accountable for protecting the data. . . . The problem is that HIPAA is antiquated . . . It's behind the times and we need to take a new approach.[69]

---

challenges in achieving EHR-interoperability: "(1) insufficiencies in health data standards, (2) variation in state privacy rules, (3) accurately matching patients' health records, (4) costs associated with interoperability, and (5) the need for governance and trust among entities, such as agreements to facilitate the sharing of information among all participants in an initiative."); *see also* Fred Pennic, *4 Challenges of Establishing EHR Interoperability*, HIT CONSULTANT (Oct. 2, 2015), http://hitconsultant.net/2015/10/02/4-challenges-of-establishing-ehr-interoperability/ [https://perma.cc/AG9Q-D9GJ].

64. Hsieh, *supra* note 51, at 189. It must be acknowledged that there are some provisions under the HITECH regulations that attempt to address the capabilities of an EHR to communicate electronically with other electronic systems. For example, HITECH requires that the EHR have the ability to e-prescribe so that prescriptions can be sent electronically to a pharmacy. 45 C.F.R. § 170.314(b)(3) (2016).

65. *See* Hsieh, *supra* note 51, at 190.

66. Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (Feb. 20, 2003). For information regarding any guidance and lack of updates since enactment of the final rule, see Dep't of Health & Human Servs., Office for Civil Rights, *The Security Rule*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/security/ [https://perma.cc/U8SF-HEAM].

67. Elizabeth Snell, *Is the HIPAA Security Rule Doing Enough for Healthcare?*, HEALTHITSECURITY (Apr. 22, 2015), http://healthitsecurity.com/news/is-the-hipaa-security-rule-doing-enough-for-healthcare [https://perma.cc/UVD3-3HEX].

68. Cynergistek, Inc. is a healthcare IT company providing security, privacy, compliance and audit, and management services for entities in the healthcare industry. *See generally* CYNERGISTEK, INC., http://cynergistek.com/ [https://perma.cc/QD42-72C2].

69. *See* Snell, *supra* note 67. "NIST" stands for the National Institute of Standards and Technology, and "ISO" stands for the International Organization for Standardization. *Id.*

Although the HIPAA security standards have not been updated since 2003, the government has consistently updated standards from the NIST with respect to cybersecurity and recently created a "crosswalk"[70] between the NIST guidance and HIPAA security regulations.[71] The NIST, now part of the U.S. Department of Commerce, was founded in 1901 to "remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals."[72] Today, the NIST's measurements support all sizes and forms of technologies, including cybersecurity.[73] In February of 2014, the NIST released its *Framework for Improving Clinical Infrastructure Cybersecurity* pursuant to an Executive Order.[74] The framework was intended "to help organizations in any industry to understand, communicate, and manage cybersecurity risks."[75] Because HIPAA has its own set of regulations regarding security of electronic health information, the goal is to identify potential gaps between HIPAA regulations and NIST guidance so that covered entities under HIPAA[76] can examine their own security programs and incorporate some of the NIST recommendations into their risk management programs.[77] The NIST is quick to point out, however, that its guidelines should not lead a provider to assume that such security provisions will necessarily be HIPAA compliant[78] or that any provider is required to abide by the guidelines.[79] Rather, the "crosswalk" should be seen as a sort of best practice that can provide guidance on supplementing the security regulations under HIPAA.[80]

---

70. A "crosswalk" is a term used to "describe a mechanism or approach to translating, comparing or moving between meta data standards . . . or converting skills or content from one discipline to another," which in this instance means a mechanism for translating or comparing the HIPAA regulations to the NIST data standards. *See* Karen Gross, *Crosswalks*, U.S. DEPT. OF EDUC. OFF. OF THE UNDER SECRETARY (May 1, 2012), https://sites.ed.gov/ous/2012/05/crosswalks/ [https://perma.cc/H2DKZFEH] (internal citation omitted).

71. CROSSWALK, *supra* note 24.

72. Nat'l Inst. of Standards & Tech., Public Affairs Office, *About NIST*, NIST.GOV, https://www.nist.gov/about-nist [https://perma.cc/E55D-KTKR].

73. *Id.*

74. *See* CROSSWALK, *supra* note 24, at 1 (citing Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013)).

75. *Id.*

76. 45 C.F.R. § 160.103 (2014).

77. CROSSWALK, *supra* note 24, at 1.

78. *Id.* at 2 (stating that the mappings are "intended to be an informative reference and do not imply or guarantee compliance with any laws or regulations").

79. *Id.*

80. *Id. See* U.S. Dep't of Health & Human Servs., *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework*, HHS.GOV,

In addition to the NIST guidance, HHS also issued guidance in July of 2016 in the form of a Q&A Fact Sheet ("Fact Sheet") for the specific purpose of describing "ransomware attack prevention and recovery from a healthcare sector perspective, including the role . . . HIPAA . . . has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack."[81] Noting that there has been a 300% increase in reported ransomware attacks since 2015, the Fact Sheet asks and answers eight questions ranging from explanations of ransomware itself to helping HIPAA covered entities understand how to undertake an analysis as to whether an attack constitutes a breach under HIPAA.[82] HHS states in the guidance that the Security Rule does contain some requirements that may "help prevent introduction of malware, including ransomware,"[83] but concedes that the Security Rule simply sets forth minimum requirements and recommends that entities implement more rigorous standards for purposes of securing Protected Health Information (PHI).[84] One of HHS' aims in releasing the Fact Sheet is to answer lingering questions regarding how such attacks should be characterized under HIPAA.[85] HHS makes clear that such attacks constitute a "security incident" under the Security Rules, thus initiating the security incident response and reporting procedures.[86] Whether ransomware attacks constitute a breach under HIPAA's Privacy Rule, however, is based upon the facts of a particular incident, according to HHS.[87] HHS recognizes that in many instances of ransomware attacks, the particular victim may be unable to determine while the system was being held captive if such data was accessed and may require an analysis

---

https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html?language =es [https://perma.cc/3XD6-BDDH].

81. U.S. Dep't of Health & Human Servs., *Fact Sheet: Ransomware and HIPAA*, HHS.GOV (July 11, 2016), http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf [https://perma.cc/U8YL-4K6Q] [hereinafter *Ransomware Fact Sheet*].

82. *Id.* at 1.

83. *Id.*

84. *Id.* at 1–2. *See also* 45 C.F.R. § 160.103 (2014) ("Protected Health Information" is defined as "(1) individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; (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 decreased for more than 50 years.").

85. *Ransomware Fact Sheet*, *supra* note 81, at 4–7.

86. *Id.* at 4.

87. *Id.*

of the particular malware algorithm to really understand whether any data was accessed.[88] Ultimately, HHS advises providers that they will have to undertake the same analysis in determining whether the breach, based on its specific facts, is reportable as a breach to those affected.[89]

B. Ransomware Attacks

Although the government has taken some measures to assure security of EHRs, over the past five or six years a number of factors have led to an environment in which these security breaches have become increasingly common. Certainly, data breaches and security concerns are not new in the healthcare industry.[90] Since HIPAA regulations first went into effect in 2003, there have been multiple reports of breaches, although until recently most breaches have been small-scale, such as stolen or lost laptops.[91] Within the last two to three years, however, smaller breaches have morphed into larger-scale HIPAA breaches, such as hackers infiltrating the networks of large health systems and insurers.[92] According to an HHS database maintained for breaches affecting more than 500 individuals, there have been 193 reported incidences of breaches as a result of "hacking/IT incident" since 2009, at least nine of which affected more than one million individuals.[93] Such breaches have included a hack into a database of almost 80 million personal consumer records at Anthem Inc., a large health insurer,[94] and a hack affecting the personal data of more than 4.5 million patients into Community Health System, a publicly traded hospital company with more than 200 hospitals in twenty-nine states at the

88. *Id.* at 6.

89. *See generally id.*

90. *See* Scannell & Chon, *supra* note 17.

91. Cindy Gallee, *The Importance of Data Encryption and Security Rules: Breaches of Electronic Protected Health Information Under HIPAA and HITECH*, 26 DCBA BRIEF 16, 18 (June 2014).

92. *See* Scannell & Chon, *supra* note 17. This is not to imply that small-scale breaches have ceased. On the contrary, there have been more than eighty breaches affecting more than 500 individuals in the first six months of 2016 for breaches unrelated to hackers or other IT incidents. *See* U.S. Dep't of Health & Human Servs., Office for Civil Rights, *Breaches Affecting 500 or More Individuals*, HHS.GOV, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=78DDA9A0C78B25921265CE8E312BC929.worker1 [https://perma.cc/YC6D-K6AJ] (based on a review of all breaches reported since 2009).

93. *Id.* (based on review of breaches in excess of one million individuals as a result of "hacking/IT incident").

94. Andrea Peterson, *2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse*, WASH. POST (Mar. 20, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/?utm_term=.ed5999920f0c [https://perma.cc/5LFM-RCPQ].

time of the incident.[95] In contrast to ransomware attacks, which seem focused on cutting off access to an electronic system, it appears that these large-scale hacks are for the purpose of obtaining the personal information contained within the records.[96] Based on the investigations of these attacks, the hackers appear to be accessing personal information on patients and insureds, such as names, addresses, birthdates, telephone numbers, and social security numbers. Significantly, not all attacks have accessed financial or medical information.[97]

Observers have identified two possible reasons for these attacks.[98] First, the data that is being accessed is the type of data frequently targeted by criminals who then sell the "hacked" data on the black market.[99] Much of the same information that can be obtained by accessing credit card information is accessible through medical records, but use of medical data by identity thieves is much more difficult to detect than data obtained through credit card theft.[100] Many of the large-scale data breaches have been traced back to individuals in China,[101] and some theorists speculate that the hackers could be working on behalf of the Chinese government in

95. Beth Kutscher & Joseph Conn, *Chinese Hackers Hit Community Health Systems; Others Vulnerable*, MOD. HEALTHCARE (Aug. 18, 2014), http://www.modernhealthcare.com/article/20140818/NEWS/308189946 [https://perma.cc/VV23-Y5B4]. Note that since the breach incident in 2014, Community Health Systems has sold off some of its hospitals, and at the time of this Article, it owned and operated 158 hospitals in twenty-two states. *See Locations*, COMMUNITY HEALTH SYS., http://www.chs.net/serving-communities/locations/ [https://perma.cc/F8SC-6ZV4].

96. *See Ransomware Fact Sheet*, *supra* note 81 (defining ransomware's defining characteristic to be that it "attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid," but noting that "hackers may deploy ransomware that also destroys or exfiltrates data").

97. *See* Kutcher & Conn, *supra* note 95.

98. Scannell & Chon, *supra* note 17; Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ [https://perma.cc/N6LC-P7BM] [hereinafter Zetter I].

99. Scannell & Chon, *supra* note 17; *see also* Peterson, *supra* note 94 ("Health organizations are targets because they maintain troves of data with significant resale value in black markets . . . and their security practices are often less sophisticated than other industries. . . . Some of the data can be used to pursue traditional financial crimes[—]like setting up fraudulent lines of credit. . . . But it can also be used for medical insurance fraud, like purchasing medical equipment for resale or obtaining pricey medical care for another person. This type of scheme is often not caught as quickly as financial fraud, experts said, and could have a lasting affect if it results in a person's medical history containing false information.").

100. Scannell & Chon, *supra* note 17 (noting that because of the longer "shelf life" of a medical record, and due to the lack of detectability by law enforcement, medical records are valued anywhere between $200 and $2,000 per record on the black market, as opposed to $1 for a credit card record).

101. *Id.*

an effort to learn how insurers and healthcare companies in the United States address healthcare challenges and population health.[102]

In contrast, the goal behind the more recent ransomware attacks, such as that against MedStar, seems to be financially driven, that is, payment of the bitcoin ransom.[103] Ransomware, which *Wired Magazine* has referred to as "digital extortion," began in about 2005 and has only grown since its inception.[104] Ransomware is defined as "malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in Bitcoin."[105] It can affect various types of computer technology, including desktop computers, laptops, and mobile phones.[106] Historically, the typical means by which ransomware attacks a system is through an email that, at first, appears legitimate, but when the recipient opens it and clicks on the attachment or a URL site, the attachment or website contains a ransomware code that infects the recipient's computer or smart phone with malicious software.[107] The malicious software "begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to."[108] Ransomware hackers have become much more sophisticated, however, and have developed techniques that bypass emails or the need for individuals to click on a link; rather, hackers can seed legitimate websites with malicious code that will infiltrate computers through known gaps in security systems.[109] Often, the recipient of the malicious software is entirely unaware of what is happening until they are unable to access the computer

---

102. *Id.* ("American investigators believe hackers in China target insurers in the US . . . to learn how medical coverage and insurer databases are set up, people familiar with the cases said. The records are also valuable for intelligence purposes. Addressing healthcare challenges has been a top priority of the Chinese government, which is facing an ageing and affluent population that is demanding better care. 'China is very interested in anything that will help them with the illnesses they are dealing with and changes in their population.'").

103. Zetter I, *supra* note 98.

104. *Id.*

105. Kim Zetter, *Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise*, WIRED (Sept. 17, 2015), https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ [https://perma.cc/D6Q7-QZMK] [hereinafter Zetter II].

106. *Id.*

107. *Incidents of Ransomware on the Rise*, U.S. FED. BUREAU OF INVESTIGATION (Apr. 29, 2016), https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise [https://perma.cc/KQ2C-WN78] [hereinafter FBI].

108. *Id.*

109. *Id.*

system or have received a ransom note from the hacker.[110] Such was the case at MedStar.[111]

Ransomware has also grown exponentially as the ability to demand *and actually collect* payment has become easier.[112] Kim Zetter of *Wired Magazine* noted,

> Many of these early [ransomware] schemes had a big drawback for perpetrators, though: a reliable way to collect money from victims. In the early days, online payment methods weren't popular the way they are today, so some victims in Europe and the US were instructed to pay ransoms via SMS messages or with pre-paid cards. But the growth in digital payment methods, particularly Bitcoin, has greatly contributed to ransomware's proliferation. Bitcoin has become the most popular method for demanding ransom because it helps anonymize the transactions to prevent extortionists from being tracked.[113]

In addition to ease of payment, ransomware attacks were further spurred by the invention of CryptoLocker.[114] CyptoLocker is software that infects a computer with a virus initially for the purpose of stealing banking credentials, but if the hacker is unable to obtain the credentials, the software installs a "backdoor" on the affected computer to extort the individual to pay money.[115] CryptoLocker was the first of its kind to use Bitcoin as the payment method, which made the payment (if and when made) almost untraceable.[116] After the invention of CryptoLocker, more than 500,000 computers were infected over a six-month time period.[117] While only a small percentage of victims paid the ransom demand, it nevertheless has become big business for hackers, with the United States Federal Bureau of Investigation (FBI) estimating in 2014 that ransom seekers made $27 million from those users who decided to pay.[118]

The FBI has issued several warnings within the past two years about the rise in ransomware attacks, warning not only individuals but businesses, government agencies, academic institutions, law enforcement

---

110. *Id.*

111. *See* Cox, *supra* note 2.

112. *See* Zetter II, *supra* note 105.

113. *Id.*

114. *Id.*

115. *Id.* (noting that CryptoLocker was invented by a hacker named Slavik).

116. Joseph Conn, *Ransomware Scare: Will Hospitals Pay for Protection?*, MOD. HEALTHCARE (Apr. 9, 2016), http://www.modernhealthcare.com/article/20160409/MAGAZINE/304099988 [https://perma.cc/JCY9-Y4C4].

117. *See* Zetter II, *supra* note 105.

118. *Id.*

agencies, hospitals, school districts, and state and local governments.[119] The FBI has further noted that with the increase in attacks, there has also been an increase in the amount of the payoffs being demanded and the damage that is being caused to the individuals, businesses, and other entities suffering from these attacks.[120] Unfortunately, CryptoLocker is now only one of several different types of malware, and the ability to guard against these attacks is becoming increasingly challenging.[121]

The latest attacks against healthcare organizations seem to be related to two specific types of ransomware, Locky and Samas.[122] The Locky virus, the same virus that infiltrated the EHRs of King's Daughter's Health in Madison, Wisconsin is hidden within emails that are opened by an unknowing individual and then moves through the system encrypting computer files, thus locking them to the user until access is granted by the ransomware attackers.[123] Samas, thought to be the likely source of the attack on MedStar, attacks certain vulnerabilities in web servers.[124] With the level of sophistication and manner in which these operations are carried out, it is clear that the individuals behind the attacks are professionals and that the healthcare industry is becoming a more common and frequent target.[125] Indeed, Beazley Breach Response Services[126] reported only twelve incidents in 2015 affecting the healthcare industry (with thirty-one ransomware attacks to other industries) but reported eighteen such attacks in just the first three months of 2016 (with twenty-two such attacks to other industries).[127] Likewise, another report

---

119. *Id.*; FBI, *supra* note 107.

120. FBI, *supra* note 107.

121. *See* Zetter II, *supra* note 105.

122. Conn, *supra* note 116.

123. *Id.*; *see also* Akanksha Jayanthi, *US, Canada Issue Joint Ransomware Alert After String of Hospital Attacks*, BECKER'S HEALTH IT & CIO REV. (Apr. 1, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/us-canada-issue-joint-ransomware-alert-after-string-of-hospital-attacks.html [https://perma.cc/2NGH-LGRJ].

124. Conn, *supra* note 116. The FBI issues two alerts to businesses in the spring of 2016 noting that the ransomware Samas (also known as MSIL) attacks servers that are "running out of date versions of a type of business software known as JBOSS," which systems are identified by the hackers utilizing a software tool known as JexBoss. Jim Finkle, *FBI Wants U.S. Businesses to Help as Cyber Extortion Gains Urgency*, REUTERS (Mar. 28, 2016), http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0WU1GB [https://perma.cc/UTX8-JGW5].

125. *Id.*

126. Beazley Breach Response Services is a specialty insurance company that provides insurance related to cybersecurity. *Beazley Breach Response (BBR)*, BEAZLEY, https://www.beazley.com/usa/specialty_lines/professional_liability/technology_media_and_business_services/beazley_breach_response.html [https://perma.cc/95PD-GATX].

127. *Id.*

from Accenture[128] estimates that by 2019 one in thirteen patients will have had their medical and personal information stolen due to healthcare provider data breaches, and that those numbers will continue to rise.[129]

This increased attention to the healthcare sector by ransomware attackers is, unfortunately, not surprising to many.[130] While HITECH has been largely successful in its goals of moving the healthcare industry into the digital age in an effort to provide better and more coordinated care, it has failed to acknowledge the culture that has risen up around the importance of information technology (IT) and the long-term investment necessary to sustain such systems.[131] In a report issued by Peer 60,[132] thirty percent of hospital executives cited "improving information security" as a concern, but more notably, eight other IT concerns were mentioned more commonly as top concerns of these executives.[133] As one critic noted,

> Many of the small- or medium-sized health care organizations do not view IT as an integral part of medical care but rather consider it as a mandate that was forced on them by larger hospitals or the federal government. Precisely due to this reason, health care organizations do not prioritize IT and security technologies in their investments and thus do not allocate required resources to ensure the security of their

---

128. Accenture is a consulting agency that provides consulting services regarding various sectors of business, including digital services and technology. *What We Do*, ACCENTURE, https://www.accenture.com/us-en/company [https://perma.cc/C3NU-NJCM].

129. Brian Kalis et al., *The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction*, ACCENTURE (2015), https://www.accenture.com/t20150723T115443__w__/us-en/_acnmedia/Accenture/ConversionAssets/DotCom/Documents/Global/PDF/Dualpub_19/Accenture-Provider-Cyber-Security-The-$300-Billion-Attack.pdf [https://perma.cc/K8QB-JVR7] (estimating that by 2019, seven million patients will have their medical information stolen, almost two million will become medical identity theft victims, and just over one million patients will have to pay out-of-pocket costs related to medical identity theft, effectively doubling the number of patients affected in 2015).

130. Monte Reel & Jordan Robertson, *It's Way Too Easy To Hack the Hospital*, BLOOMBERG BUS. WEEK (Nov. 2015), http://www.bloomberg.com/features/2015-hospital-hack/ [https://perma.cc/5429-QZLJ] (citing medical devices and lack of security in connection with such devices as a major issue and a gateway for malware into hospital systems).

131. Yaraghi, *supra* note 55.

132. Peer60 is a marketing research company that provides services for various industries, including healthcare. *See Reaction*, PEER60, https://www.peer60.com/solutions/ [https://perma.cc/QPE2-XP5P].

133. *See* Rev360 Editor, *Cybersecurity for Hospitals—the Road Ahead* (Jan. 28, 2016), http://revenue360.net/revenue360_modules/address_demographic_validation/cybersecurity-for-hospitals-the-road-ahead/ [https://perma.cc/7VWB-LPWH] (citing the Peer60 report which noted the following top challenges that the organization needs to address: 64% said "managing switch to value based reimbursement models"; 56% said "coordinating care"; 54% said "managing patient populations"; 48% said "patient engagement"; 47% said "shortages of physicians and nurses"; 36% said "managing data"; 33% said "regulatory compliance"; and 31% said "meaningful ROI on IT purchases").

> IT systems which makes them especially vulnerable to privacy breaches . . . . When it comes to data protection, big technology companies are the war ships, and hospitals are small rubber dinghies in a sea of hacker sharks. Since IT has not historically been an integral part of medical services, hospitals have lagged behind other industries on investing in security technologies and attracting top IT talents and thus became especially weak and vulnerable to IT attacks.[134]

Other critics have noted similar concerns related to the culture of the healthcare industry when it comes to investment in technology infrastructure and maintenance.[135] Already required to make a substantial capital investment in an electronic system, many providers are unwilling to incur the additional expenses associated with maintenance and updates to such system, much less adopt additional security measures beyond those required by HIPAA, such as backup systems or other security measures adopted by more technologically sophisticated industries.[136] And yet, even if a healthcare system has invested the capital and taken all necessary actions to protect such data with the most up-to-date technology and highest security, some argue that cybersecurity will forever remain challenging and potentially elusive because human error remains one of the biggest risks.[137] This risk will continue to be an issue, even with education and training, as malware attackers continue to refine their skills.

Thus, it appears that the healthcare industry is in the midst of a "perfect storm" of circumstances that make it especially vulnerable to these types of attacks. These circumstances include: (a) the industry, as a whole, adopted the use of EHRs in a very rapid timeframe, with a focus on compliance with HIPAA privacy and security regulations drafted for the purpose of preventing disclosure of sensitive information, not guarding

---

134. Yaraghi, *supra* note 55.

135. Regina E. Herzlinger, *Why Innovation in Health Care is So Hard*, HARV. BUS. REV., May 2006, https://hbr.org/2006/05/why-innovation-in-health-care-is-so-hard (noting after the implementation of HIPAA, but prior to the HITECH standards, that the healthcare industry is "near the bottom of the ladder in terms of IT spending and uniform data standards").

136. Stacy Cowley & Liam Stack, *Los Angeles Hospital Pays Hackers $17,000 After Attack*, N.Y TIMES (Feb. 18, 2016), https://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html?_r=0 ("Health care organizations seem to be particularly vulnerable to hacking attacks because they have been slower to embrace sophisticated backup systems and other security measures than other industries, like financial services, said Katherine Keefe, the head of breach response services at Beazley, an insurance company.").

137. John Halamka, *The State of Information Security 2015*, LIFE AS A HEALTHCARE CIO BLOG (Dec. 9, 2015, 3:00 AM), http://geekdoctor.blogspot.com/2015/12/the-state-of-information-security-2015.html [https://perma.cc/V6KG-D92X] (citing examples of most common entry of malware into a system).

against outside attacks;[138] (b) malware and ransomware attacks have become increasingly more prevalent as hackers,[139] the software tools available to them,[140] and the ability to collect payment through Bitcoin have become more sophisticated and exceedingly difficult to police;[141] (c) unlike in a retail sector, for example, health care providers blocked by ransomware from accessing their EHR can result in very serious public health and patient safety concerns that might lead many in the industry to consider paying the ransom due to the dire consequences caused by lack of access to their EHR systems;[142] and (d) the health care industry culture, perhaps as a result of the rapid adoption of EHR as necessitated by federal regulations and the costs associated with such systems, does not appear to have yet embraced the need for security regulations outside of mere HIPAA compliance.[143] While increased vigilance and greater security protections are obvious responses, one questions whether such responses are truly enough to assure greater protection of patient data and the operation and safety of hospitals, doctors' offices, and other healthcare facilities that are so vulnerable to these attacks.

II. CURRENT LEGAL AND BUSINESS RESPONSES

A. Computer Fraud and Abuse Act

Although the HIPAA Security Rule is perhaps the primary source for healthcare entities seeking to protect data from cyberattacks, there are other federal laws that have been enacted in order to protect personal data, such as health records, from hackers.[144] Originally enacted as part of the Comprehensive Crime Control Act of 1984,[145] the Computer Fraud and Abuse Act (CFAA) was the first federal law to address computer crime.[146] Prior to the CFAA, prosecutors relied on mail and/or wire fraud laws for

138. *See* Yaraghi, *supra* note 55.

139. FBI, *supra* note 107.

140. Zetter II, *supra* note 105.

141. *See* FBI, *supra* note 107.

142. *See* Winton, *supra* note 15; Cox, *supra* note 2.

143. *See* Snell, *supra* note 67.

144. *See* Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 151–52 (2014).

145. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified at 18 U.S.C. § 1030). Note that, when enacted, the law was referred to as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, but was shortened to the Computer Fraud and Abuse Act after an amendment to the law in 1986.

146. United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991).

most computer-related crimes.[147] While the first version of the CFAA was rather limited in scope,[148] the law was extensively amended in 1986 and has since been amended numerous times.[149] As amended, the CFAA punishes individuals who knowingly, intentionally, and maliciously transmit code or access protected computers and such action causes harm, including attacks against hospital EHRs.[150] The penalties for violating the CFAA can be quite steep, and can result in a fine, imprisonment for not more than ten years, or both for a first offense in which the individual "intentionally causes damage without authorization to a protected computer."[151] The CFAA also imposes penalties for an individual who "intentionally accesses a protected computer without authorization and as a result of such conduct, recklessly causes damage," which can result in a fine, imprisonment up to five years, or both.[152]

While the penalties are potentially steep and the language of the CFAA is quite broad in its application,[153] most of the prosecutions under

147. Paul J. Larkin, Jr., United States v. Nosal*: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIR. REV. 257, 262 (2012).

148. For example, under the first version of the law, enacted in 1984, only federal government computers and computers owned by large financial institutions were subject to the law in an effort to provide the Secret Service with authority to investigate certain computer crimes. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976. Likewise, earlier versions of the law required an actual interstate or foreign communication. *See* 18 U.S.C. § 1030(a)(2)(C) (2007).

149. *See* U.S. DEP'T OF JUST. OFF. LEGAL EDUC., PROSECUTING COMPUTER CRIMES (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/H7HR-TXLV]; *see also* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213; Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 2097, enacted as Title XXIX of the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 2013-322, 108 Stat. 1796; Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272; Identity Theft Enforcement and Restitution Act of 2008, codified as Title II of the Former Vice President Protection Act of 2008, Pub. L. No. 110-326, 122 Stat. 3560 (2008).

150. 18 U.S.C. § 1030(a)(5)(A), (B) (2012).

151. 18 U.S.C. § 1030(a)(5)(A) (2008).

152. 18 U.S.C. § 1030(c)(4)(A)(i) (2008).

153. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) (finding that amendments to the CFAA and congressional reports indicate that the statute was meant to be applied broadly). Note, however, that certain provisions of the CFAA that include specific language related to when an employee is using a computer "without authorization" have been interpreted rather narrowly by certain circuits and broadly by others. *See* United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); *and* EF Cultural Travel BV. v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (all holding that an employee could be in violation of the CFAA if the employee accessed information on the computer without permission, even if the employer did not take means to make such information inaccessible). *But see* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) *and* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (each holding that "without authorization" under the CFAA is limited to situations where the employee no longer has access to the information, as such provision is intended for "outside" hackers).

the CFAA have been focused on individuals such as employees or independent contractors, and much of the defense centers around whether such individual had "authorization" under the statute to access the protected computer.[154] In fact, there have been few instances of prosecution under the CFAA of unknown criminal hackers.[155] One of the reasons that hackers have been less likely to be prosecuted under the CFAA is because of the complexities and challenges associated with identifying and apprehending a hacker, especially individuals located in foreign jurisdictions.[156] Computer networks in general are vastly complicated, consisting of the use of various private networks (such as a virtual private network (or VPN) that encrypts the data sent over such network and protects the applicable internet protocol (IP) address).[157] Healthcare entities use such VPN networks to ensure protection of data that may be accessed remotely by employees or agents.[158] As Larry Greenemeier points out, however, when it comes to hackers, this can become even more complex:

> Cyber attackers use viruses, worms and other malware to take control of Internet servers or even personal computers, creating a network of

154. *See generally* U.S. DEP'T OF JUST., *supra* note 149, at 6–12; Larkin, *supra* note 147. Perhaps the most notable prosecution under the CFAA was the conviction of Aaron Swartz, a twenty-six year-old, self-described internet activist who was prosecuted under the CFAA after he downloaded a large number of articles from a website called JSTOR that contains academic documents. While Swartz had a JSTOR account, he downloaded nearly the entire JSTOR library to a computer at the Massachusetts Institution of Technology for the purpose of allowing others to access it ("open data"). Swartz was charged with eleven felony violations under the CFAA and faced up to thirty-five years in prison. He committed suicide before his trial. John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES (Jan. 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html?r=0. One of the key questions in the case was whether or not Swartz had "authorization" under the CFAA. *See* James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCI. AM. (Aug. 16, 2013), http://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/ [https://perma.cc/F3HZ-BSPA] (arguing that the CFAA has been overly prosecuted and needs to be reformed).

155. *See* Wellington, *supra* note 144 (citing United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6004208 (N.D. Tex. Nov. 5, 2012); United States v. McGraw, No. 3:09-CR-0210-B, 2012 WL 6013258 (N.D. Tex. Dec. 3, 2012) in which Jesse McGraw was convicted under the CFAA in connection with accessing a hospital network and downloading malicious software).

156. Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), http://www.scientificamerican.com/article/tracking-cyber-hackers/ [https://perma.cc/3ELM-WZJT].

157. *Id.* ("By way of example, Nicol points out that he uses a virtual private network that connects to a proxy server before connecting him to the Internet. This enables him to encrypt data he sends over the network and protect the identity of his own Internet protocol (IP) address. 'I do this to thwart information harvesting that commercial Web sites usually have,' he adds.").

158. SSL Servs. LLC v. Citrix Sys., Inc., 769 F.3d 1073, 1078 (Fed. Cir. 2014) (defining a "virtual private network" as "system for securing communications between computers over an open network such as the Internet").

> "zombie" computers (also called botnets) under their control that they can use to launch their attacks. As a result, an attack may appear to come from a particular server or computer, but this does not mean the attack originated at that device, . . . [and] often a string of proxies located in different countries are used in an attack, "greatly complicating the legal process of trying to piece it all together."[159]

Hackers have the ability to not only encrypt their identity through software or "mask" their IP addresses but also leave "false flags" that will implicate other individuals, which leads one to believe that the hacker was an entirely different person.[160] Thus, hackers are, by design, almost impossible to identify with certainty.[161]

Independent of the challenges in simply locating a particular individual or network of individuals who may be responsible, there are various jurisdictional issues created by the fact that many hackers hail from locations outside the United States.[162] Historically, China has been a particularly common place for hackers, but attacks have also originated in Russia, Eastern Europe, the Middle East, and various Western countries.[163] With origination of these attacks in various countries, one of the main issues is attributing the particular cyberattack to a particular individual or group and then obtaining cooperation from other law enforcement officials in other countries (assuming such countries have similar laws that might criminalize cyber or computer fraud).[164] While there has been some

---

159. Greenemeier, *supra* note 156. Duncan Hollis has described a similar scenario in more real life terms:

> Imagine Twitter falls victim to a cyberattack. Twitter's systems keep a record . . . of every IP address visiting its site, which allows it to identify the attacker's IP address. It can then use the IANA (Internet Assigned Numbers Authority) database to identify which internet service provider (ISP) was assigned to that IP address. If that ISP keeps good records, it could tell Twitter to which computer's modem it had assigned that address. . . . ISPs regularly empty out their logs. . . . Thus, sourcing requests have to happen quickly; otherwise, any evidence to identify perpetrators is gone. Even where there are records, the IP address might go with a corporate account, numbering thousands of users. Or, the trial might end sooner if it goes to a coffee house that gives users free access, no questions asked. Assuming Twitter can actually trace the IP address back to a single user, it might find that the computer had been captured. . . . In effect, attackers can 'launder' the packets so that the attack's true origins will be difficult, if not impossible, to find.

Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 398–99 (2011).

160. Hollis, *supra* note 159, at 397 ("The most sophisticated cyber exploitations may never be discovered. A high-level attack might be attributed to mere computer error. This situation is unlikely to change anytime soon; it is a systematic aspect of the Internet, not a simply problem to be fixed.").

161. *See id.*

162. Joseph Menn, *Analysis: The Near Impossible Battle Against Hackers Everywhere*, REUTERS (Feb. 24, 2013, 3:04 AM), http://www.reuters.com/article/us-cybersecurity-battle-idUSBRE91N03520130224 [https://perma.cc/MMB7-E46R].

163. *Id.*

164. Hollis, *supra* note 159, at 392.

international cooperation with respect to cyberattacks, including the Convention on Cybercrime, which is now joined by twenty-nine European countries and the U.S.,[165] such laws do not necessarily include attacks coming from a military or intelligence agency, or individuals or groups acting pursuant to a lawful government authority.[166] This exclusion includes activities that may be done for investigation purposes or to protect national security, which has led to a lack of clarity regarding when the activity of a country might otherwise have qualified as a cybercrime.[167] Even with uniformity in the laws and some international cooperation regarding enforcement, anonymity, and the ability to actually identify the hackers remains elusive.[168]

B. Cybersecurity Information Sharing Act

Given some of the challenges in attempting to apprehend and prosecute cyber attackers, there are other statutory responses that endeavor to aid in exchange of data to facilitate more coordinated and robust defenses. For example, in response to the recent increase in ransomware attacks across all industries and increasing concerns with cybersecurity generally the U.S. Congress enacted the Cybersecurity Information Sharing Act (CISA) in 2015.[169] Unlike the CFAA, which is focused on enforcement, the CISA is instead centered on the idea that cybersecurity threats, especially those related to national security, may potentially be thwarted or at least diminished by greater sharing of threat information.[170] The sharing of information is entirely voluntary under the CISA, but the intention is to address what has been a major barrier with the sharing of this data. This would assuage fears on the part of companies that monitoring and implementing defensive mechanisms or sharing the data with others could result in liability under any number of laws,[171] including

---

165. Convention on Cybercrime, Council of Europe, Nov. 23, 2001, C.E.T.S. No. 185, http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185.

166. Hollis, *supra* note 159, at 393.

167. *Id.* at 393–94.

168. *Id.* at 397.

169. Cybersecurity Information Sharing Act (CISA) was passed as part of the Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (Dec. 18, 2015).

170. Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [https://perma.cc/L7HT-L5WG].

171. There is criticism regarding the CISA that it does not do enough to protect personal data because it shares information and that the sharing of information with the federal government could be a threat to civil liberties, even if the law does exempt companies from liability concerns. *See* Everett Rosenfeld, *The Controversial "Surveillance" Act Obama Just Signed*, CNBC (Dec. 22, 2015, 12:34 PM), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html

the Electronic Communications Privacy Act,[172] the Freedom of Information Act (FOIA),[173] antitrust laws,[174] privacy laws (such as HIPAA and HITECH),[175] and potentially a waiver of attorney–client privilege or similar protections.[176]

In order to guard against potential application of these laws, the CISA contains a number of provisions that endeavor to accomplish this goal. First, the CISA contains an express federal preemption pursuant to which the CISA "supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under [the CISA]."[177] This preemption is limited, however, by any other law "concerning the use of authorized law enforcement practices and procedures."[178] In addition to this express preemption, there are a number of other provisions that provide additional protections (and encouragement) for companies to share information regarding cyberattacks. Specifically, the CISA permits a company to "monitor" and "operate defensive measures" for cybersecurity purposes on its own systems or on a third-party system, with authorization from such third party,[179] thus enabling companies to monitor their systems without the potential liability concerns of infringing on privacy rights of individuals.[180]

Second, companies are permitted, notwithstanding any provision of law to the contrary, to share information with or receive information from federal, state, or local governments in connection with "cyber threat

---

[https://perma.cc/KL8N-87GV]; Graeme Caldwell, *Why You Should Be Concerned About the Cybersecurity Information Sharing Act*, TECH CRUNCH (Feb. 7, 2016), https://techcrunch.com/2016/02/07/why-you-should-be-concerned-about-cisa/ [https://perma.ccWZ89-ZHVM].

172. 18 U.S.C. §§ 2510–2522 (2002) (extending government restrictions on wire taps to electronic data used by a computer).

173. 5 U.S.C. § 552 (2016) (allowing individuals the right to access certain information/documentation held or controlled by the United States government).

174. 15 U.S.C. §§ 1–7 (2004) (prohibiting competitors or would-be competitors from agreeing or conspiring to agree to restrict trade).

175. The Privacy Rule and Security Rule are combined in the HIPAA Administrative Simplification Regulations found at 45 C.F.R. §§ 160, 162, and 164 (2013).

176. Karp, *supra* note 170. Please note that attorney–client privilege and requirements for waiver of such privilege are matters of state law and will vary from state to state. In general, there is a fear that reporting information regarding cyberattacks while still investigating the origins of the attack and the information that was accessed as part of such cyberattack may waive any privilege that exists.

177. 6 U.S.C. § 1507(k)(1) (2015).

178. 6 U.S.C. § 1507(k)(2) (2015).

179. 6 U.S.C. § 1503(a)(1)(A)–(D); 6 U.S.C. § 1503(b)(1)(A)–(C) (2015).

180. *Cybersecurity Information Sharing Act*, CYBERTREND (Dec. 10, 2015), https://www.cybertrend.com/article/19423/cybersecurity-information-sharing-act [perma.cc/57Y6-HL3X].

indicators"[181] or "defensive measures,"[182] so long as such measures are for cybersecurity purposes.[183] As alluded to above, because of the application of various existing laws and fears regarding the sharing of personal data, companies have been reticent to share any information regarding cyberattacks or cyber threats.[184] Congress surmises, however, that such information would be very helpful in preventing attacks and identifying attackers because it would enable a government authority to develop means to prevent common schemes and to recognize the markers and "signatures" of common hackers, thus making them easier to identify.[185] Although the law provides for preemption, in an attempt to maintain some of the original intent of the various privacy laws in place, the CISA requires that companies remove any information that is not directly related to a cybersecurity threat and that the company knows to be personal information identifying a particular person.[186] Lastly, so long as all of the provisions for sharing under the CISA are followed, the CISA provides protections against liability in connection with data sharing,[187] prosecution

---

181. The statute defines cyber threat indicator as

> information that is necessary to describe or identify- (A) malicious reconnaissance . . . (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability . . . (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident . . . (G) any other attribute of a cyber security threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof.

6 U.S.C. § 1501(6) (2015).

182. A "defensive measure" is defined as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability." 6 U.S.C. § 1501(7)(A) (2015).

183. *Id.*

184. U.S. DEP'T OF HOMELAND SEC. & DEP'T OF JUST., GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf [https://perma.cc/5Q7K-RWSM] [hereinafter GUIDANCE].

185. *Id.*

186. 6 U.S.C. § 1503(d)(2)(A)–(B) (2015).

187. 6 U.S.C. § 1505(b)(1) (2015); 6 U.S.C. § 1505(c)(1)(B)(ii) (2015) (protecting against liability in any court against any private entity for the sharing or receipt of a cyber threat indicator or defensive measure, so long as shared through the Department of Homeland Security process).

under antitrust laws,[188] attorney–client privilege waiver concerns,[189] liability related to disclosure of proprietary information,[190] application from FOIA provisions,[191] and use of information to regulate other lawful activity.[192]

1. Healthcare Task Force

Perhaps recognizing both the extensive privacy concerns and the lack of readiness and preparedness of the healthcare industry in combating cyberattacks, the CISA contains a specific section relating to the healthcare industry and stresses the need for increased vigilance in this sector.[193] Under Section 1533 of the CISA, HHS is required to issue a report divisions within one year from the date of enactment on its preparedness to respond to cybersecurity threats, including a statement regarding who will lead and coordinate the efforts and how divisions and subdivisions[194] will divide responsibilities and communicate across.[195] Additionally, CISA directed HHS to convene a task force made up of healthcare industry stake holders, cybersecurity experts, and others as determined by other agencies or the Secretary of HHS for the purpose of planning a single system in which the federal government and those in the healthcare industry can share information regarding cybersecurity threats and also make recommendations for protections for network medical

---

188. 6 U.S.C. § 1503(e)(1) (2015) (limiting such waiver only if the sharing of information is for the purpose of preventing, investigating, or mitigating threats). It should be noted, however, that Section 1507(e) of the statute expressly states that the antitrust exemption set forth in Section 1503 shall not "be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning." 6 U.S.C. § 1507(e) (2015). Thus, the only exemptions under antitrust law appear to be limited to those activities that fall outside *per se* violations of the Sherman Act or involve the sharing of information that leads to *per se* violations. 6 U.S.C. § 1507 (2015).

189. 6 U.S.C. § 1504(d)(1) (2015) (waiving attorney–client privilege and related legal protections, including trade secrets, but limited only for sharing under the CISA—and not to state or local governments or other third parties).

190. 6 U.S.C. § 1504(d)(2) (2015) (noting that proprietary information will not be further disclosed so long as the disclosing entity designates such information as proprietary).

191. 6 U.S.C. § 1504(d)(3) (2015).

192. 6 U.S.C. § 1504(d)(5)(D)(i) (2015) (prohibiting use of any information shared for the purpose of regulating (including an enforcement action) lawful activities of a private party).

193. 6 U.S.C. § 1533 (2015).

194. HHS has eleven operating divisions, eight agencies within the U.S. Public Health Service, and three human services agencies. For a complete list, see *HHS Agencies & Offices*, HHS.GOV, http://www.hhs.gov/about/agencies/hhs-agencies-and-offices/index.html [https://perma.cc/SN69-9ZLA].

195. 6 U.S.C. § 1533(b) (2015).

devices and EHRs.[196] Recognizing that the healthcare industry can likely utilize existing resources from industries that already have highly developed security protection systems and capabilities, the task force is specifically instructed to "analyze how industries, other than the healthcare industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries."[197] The task force is required to complete its task within one year, and it has sixty days after its termination to disseminate its findings to the healthcare industry for purposes of utilizing recommendations by healthcare entities.[198] HHS has published little information about its progress, only naming the members of the task force—made up of members representing hospitals, insurers, patient advocates, security researchers, pharmacy and pharmaceutical companies, medical device manufacturers, health information technology developers and vendors, and laboratories—and noting the dates on which the task force held its four in-person meetings (and some periodic teleconferences with tasks), which were to be completed by March 2017.[199] Thus, Congress and other security experts appear to acknowledge that the healthcare industry is particularly vulnerable and exposed in terms of its capacity and ability to deal with and combat cybersecurity issues.[200]

2. Federal Guidance

Pursuant to CISA requirements, HHS and the U.S. Department of Justice (DOJ) issued guidance on February 16, 2016 and published an updated version of such guidance on June 15, 2016 (collectively, the "Guidance").[201] The Guidance was intended to assist private entities in understanding how information under CISA should be shared with the federal government.[202] The Guidance acknowledges that while the CISA does permit an entity to share information for cybersecurity purposes notwithstanding any other provision of law (including HIPAA and HITECH), it does nevertheless require the removal of any information that

196. 6 U.S.C. § 1533(c) (2015).

197. 6 U.S.C. § 1533(c)(1)(A) (2015).

198. 6 U.S.C. § 1533(c)(2) & (3) (2015).

199. *Care Industry Cybersecurity Task Force*, PUB. HEALTH EMERGENCY, http://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx [https://perma.cc/M842-TGWD]. Note that the in-person meetings will be open to the public, but the teleconferences in between are intended for administrative issues only and will not be open to the public. *Id.*

200. *Id.* (noting that "healthcare data may be used for a variety of nefarious purposes, including fraud, identify theft, and disruption of hospitals systems" and that leaving such systems unprotected could cause a risk to patient safety and thus should be afforded the highest level of care).

201. GUIDANCE, *supra* note 184.

202. *Id.*

it knows to be personal or that identifies a particular individual who is not directly related to a cybersecurity threat.[203] Highlighting particularly sensitive information where this might most frequently arise, there is specific reference in the Guidance to, among other sensitive information, PHI.[204] The Guidance states:

> [S]haring [certain sensitive categories of information] in a form that constitutes or includes personal information of a specific individual or information that identifies a specific individual may not be necessary. For instance, while sharing the medical condition of a particular individual targeted for a phishing attack is unlikely to be useful or directly related to a cybersecurity threat, sharing an anonymized characterization of the cyber threat may have utility.[205]

Thus, the Guidance clarifies that the expectation of the federal government is that the information that is shared is "technical information that describes the attributes of a cybersecurity threat that generally need not include various categories of information that are considered sensitive."[206] Finally, the Guidance highlights the various processes that can be utilized to share the data under the CISA, including an "Automated Indicator Sharing" (AIS) system,[207] submission of information by completing a web form on the Department of Homeland Security website, email submissions through the National Cybersecurity and Communications Integration Center (through a web-based portal), or through the Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations.[208] These centers are private organizations that will share the information with the Department of Homeland Security on behalf of the disclosing entity.[209] Given the report required to be issued by HHS and the goals and purpose of the task force for healthcare, it is not entirely clear if healthcare entities wishing to report under the CISA will continue to report by the methods set forth in the

---

203. *Id.* at 8.

204. *Id.* at 9–10 (mentioning human resource information, consumer information/history, education history, financial information, property ownership information, and information identifying children under the age of 13).

205. *Id.* at 8.

206. *Id.* at 8–9.

207. *Id.* at 13. This system enables timely exchange of data in a secure manner, utilizing the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), which requires the user to have TAXII capabilities that communicate with the government's TAXII servers.

208. *Id.* at 13-14.

209. *Id.* There are other means of sharing set forth in the Guidance, but only the sharing mechanisms set forth above will enable the entity to access the liability and waiver protections set forth under the CISA. *Id.* at 15.

Guidance or if there will be an entirely different process or procedure established that is uniquely designed for the healthcare industry.[210]

3. CISA Criticisms and Challenges

While the intention of the CISA was to ease communication between government and companies when it comes to cyberattacks in order to potentially combat and prevent them, there are critics of the law who are concerned that, despite attempts to the contrary, the statute will compromise privacy concerns.[211] Indeed, it took more than four years for the bill to be enacted into law, in large part because of the very strong opposition by privacy experts and civil libertarians, who argued that the broad language in the law would provide the government with access to sensitive information from private entities and could allow use of the information for other purposes.[212]

Still other critics believe that this law does not go far enough to prevent these attacks.[213] These critics are concerned that, because sharing information is entirely voluntary, companies do not have sufficient incentives or motivation to report cyberattacks and cyber threats any more than they did previously.[214] Additionally, there are concerns that any response that can be generated or created as a result of the information sharing will be too little, too late.[215] As Abigail Tracey stated,

> Many argue that cybercrime evolves at a rate that not only outpaced the Senate's legislation but that makes the sharing of information

---

210. *See* Joseph Conn, *Federal Task Force Takes on Healthcare Cybersecurity*, MOD. HEALTHCARE (Apr. 16, 2016), http://www.modernhealthcare.com/article/20160416/MAGAZINE/304169890 [https://perma.cc/MPK6-8FSK].

211. *See* Caldwell, *supra* note 171 ("The thing is, critics saw that bill as [a] way for government agencies to more easily keep tabs on Americans without their knowledge. CISA was derided by privacy advocates and tech titans alike. . . . In other words, organizations like the NSA and CIA now have even more government protections allowing them to play fast and loose with personal privacy. And our private information—already clearly at risk, given the large quantity of data breaches of late—is now even more freely available.").

212. Brett V. Newman, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 U. ILL. J.L. TECH. & POL'Y 437, 447–48 (2015) (discussing privacy concerns and other challenges with passing the Cybersecurity Information Sharing Act of 2014).

213. Jay Shelton, *Cybersecurity Information Sharing Act—Is it Enough?*, ASSURANCE (Dec. 7, 2015), http://www.assuranceagency.com/blog-post/cybersecurity-information-sharing-act-is-it-enough [https://perma.cc/DFU4-WGK4] ("While most agree that CISA is a good start, many question if the bill will go far enough in providing consumer data protections against network breaches.").

214. *Id.*

215. Abigail Tracy, *The Problems Experts and Privacy Advocates Have with the Senate's Cybersecurity Bill*, FORBES (Oct. 29, 2015, 8:43 AM), http://www.forbes.com/sites/abigailtracy/2015/10/29/the-problems-experts-and-privacy-advocates-have-with-the-senates-cybersecurity-bill/#1729c3f430fc.

> across companies [sic] effectively useless because in many cases by the time this happens, it is too late for corporations to defend themselves. "Hackers are changing their methodologies in milliseconds. Information sharing is going to take days, weeks, and months. Will this idea keep up with the pace of sophisticated hackers? That is the question that needs to be asked."[216]

Although one year's time for formation of a task force and issuance of its report is rapid speed relative to government processes, the movement of cyberattacks and the necessity to implement corresponding security measures will likely far outpace the thoughtful process currently underway.[217] In response to critiques that the new law is not responding decisively or rapidly enough, supporters, including the College of Healthcare Information Management Executives and Healthcare Information and Management Systems Society, contend that, at a minimum, the law provides *one* resource that will direct the healthcare industry to a set of best practices for cybersecurity.[218] Further, supporters argue that any law needs to remain voluntary until it is known what sorts of guidelines or methods would be effective in combating cybercrime.[219]

C. Current State of the EHR Industry

The lack of consistent standards and best practices in the EHR industry is caused at least in part by the current state of such industry.[220] One notable obstacle in establishing optimal security measures for purposes of guarding EHRs against hackers and ransomware attacks is the sheer number of EHR companies and EHR systems.[221] In 2013, *Medical*

---

216. *Id.* (quoting Craig Newman, an expert on cyber law and chair of the Privacy and Data Security practice at Patterson Belknap Webb & Tyler LLP).

217. David Harlow, *CISA: Big Brother is Watching*, HEALTHBLAWG (Dec. 22, 2015), http://healthblawg.com/2015/12/cisa-big-brother-is-watching.html [https://perma.cc/4MN7-29HB] ("The notion of analyzing cybersecurity threats at one point in time via a task force that will sunset out of existence after delivering its report simply is not a realistic response to the dynamic nature of the threat environment today.").

218. John Frank, *Don't Expect Legislative Defenses Against Cyberattacks Anytime Soon*, MED. ECON. (Apr. 10, 2016), http://medicaleconomics.modernmedicine.com/medical-economics/news/don-t-expect-legislative-defenses-against-cyberattacks-anytime-soon?page=0%2C1 [https://perma.cc/PWE7-Z3RQ].

219. *Id.*

220. HENRY ET AL., *supra* note 32 (noting that while the number of providers adopting an EHR have greatly increased, there remains variability with the adoption of functionalities and use of such EHRs).

221. *See* Ryan Shay, *EHR Adoption Rates: 19 Must-See Stats*, PRACTICE FUSION: PRACTICE FUSION BLOG (Jan. 1, 2016), http://www.practicefusion.com/blog/ehr-adoption-rates/ [https://perma.cc/39FE-PVKM] (noting approximately 1,100 EHR vendors currently, which is double the amount that existed four years ago).

Economics noted that the government's best estimate was that there were 729 companies offering certified EHR systems for medical providers.[222] *Medical Economics* stated, however, that even the government estimates are difficult to judge because basic financial information about public and private companies is difficult to garner, and it speculated that the industry is likely to witness consolidation or closure of weaker EHR companies.[223] Just two years after the report by *Medical Economics*, the number of EHR vendors has actually increased, and as predicted, some of the consolidation predicted appears to be taking root, at least in terms of market share.[224] For example, more than 50% of the market share for individual healthcare professionals is occupied by just five EHR companies (Epic Systems, Allscripts, eClinicalWorks, NextGen Healthcare, and GE Healthcare) and more than 60% of the market share for hospitals is comprised of just three EHR companies (Cerner, MEDITECH, and Epic Systems).[225] All of this information is important and impactful when considering the EHR landscape because providers do not want to have to make the costly and

222. Daniel R. Verdon, *Top 100 EHRs: Why Understanding a Company's Financial Performance Today May Influence Purchasing Decisions Tomorrow*, MED. ECON. (Oct. 25, 2013), http://medicaleconomics.modernmedicine.com/medical-economics/content/tags/ehr/top-100-ehrs-why-understanding-company-s-financial-performance-to [https://perma.cc/7HPJ-4FP2]. It should be noted that Verdon's article was reporting data from 2013, prior to when most of the "meaningful use" regulations were mandatory. Verdon acknowledged that "some companies won't be able to clear the technological and regulatory hurdles of the government's 2014 incentive program, conversion to the International Classification of Diseases-10th revision (ICD-10) or the development costs to make it happen." *Id.*

223. *Id.*

224. *See* Office of the Nat'l Coordinator for Health Info. Tech., *Quick-Stats: Certified Health IT Vendors and Editions Reported by Ambulatory Health Care Professionals Participating in the Medicare EHR Incentive Program*, HEALTH IT DASHBOARD, HEALTHIT.GOV (July 2016), https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Professionals.php (noting, "As of July 2016, 632 vendors supply certified health IT to 337,432 ambulatory primary care physicians, medical and surgical specialists, podiatrists, optometrists, dentists, and chiropractors participating in the Medicare EHR Incentive Program"). This compares to "175 certified health IT vendors [that] supply certified health IT to the 4,474 non-federal acute care hospitals, including Critical Access hospitals, participating in the Medicare EHR Incentive Program." Office of the Nat'l Coordinator for Health Info. Tech., *Quick-Stats: Certified Health IT Vendors and Editions Reported by Hospitals Participating in the Medicare EHR Incentive Program*, HEALTH IT DASHBOARD, HEALTHIT.GOV (July 2016), https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Hospitals.php [https://perma.cc/V6S6-Z2X6].

225. Helen Gregg, *50 Things to Know About Epic, Cerner, MEDITECH, McKesson, athenahealth and Other Major EHR Vendors*, BECKER'S HEALTH IT & CIO REV. (July 14, 2014), http://www.beckershospitalreview.com/healthcare-information-technology/50-things-to-know-about-epic-cerner-meditech-mckesson-athenahealth-and-other-major-ehr-vendors.html [https://perma.cc/T843-93EW]. Becker's Health IT Review noted in 2014 that just ten EHR companies account for ninety percent of the total market.

disruptive EHR transition more than once.[226] Although providers are loathe to change their existing EHR systems, having many smaller companies (with fewer clients) in the market can lead to financial instability within such smaller companies, leading to an increase in mergers, closure, or bankruptcy.[227] This instability can also hinder advancement and development of technology.[228] Such challenges have caused many providers to incur the cost of a challenging EHR transition more than once.[229] When providers are faced with a second or third transition, they will typically seek out larger EHR companies to avoid the same difficulties again.[230] Such instability in the market and movement between systems can potentially exacerbate healthcare industry vulnerabilities.[231]

The size of the EHR market and the potential consolidation has also led to other market challenges, such as an increasing trend toward the involvement of EHR companies in malpractice lawsuits and other lawsuits related to patient safety.[232] While the number of malpractice lawsuits remains small at approximately 1%, the frequency has been increasing in recent years, doubling from 2013 to 2014.[233] Many of these lawsuits have arisen out of errors in patient files that were the result of issues with a system's EHR, including "faulty voice-recognition software; [m]isinterpretation of EHR drop-down menus; [r]eliance on outdated or incorrect records; and [t]ypos that led to medical errors."[234] According to

---

226. *See* Michael McBride, *Understanding the True Costs of an EHR Implementation Plan*, MED. ECON. (July 25, 2012), http://medicaleconomics.modernmedicine.com/medical-economics/news/modernmedicine/modern-medicine-feature-articles/understanding-true-costs-ehr-?page=full (highlighting all of the direct and indirect-and sometimes hidden-costs of implementing a new EHR system).

227. *See* Gregg, *supra* note 225.

228. *Id.* ("Recently, the EHR market has seen an infusion of providers seeking replacements for their current systems. Surveys suggest between 12 and 30 percent of providers are dissatisfied with their EHR. Girish Navani, CEO and co-founder of eClinicalWorks, said in 2013 more than half of his company's new clients came from another vendor.").

229. *Id.*

230. *See id.*

231. *See* Sittig & Singh, *supra* note 38, at e1044; David W. Bates et al., *A Proposal for Electronic Medical Records in U.S. Primary Care*, 10 J. AM. MED. INFORMATICS ASS'N 1, 6–7 (2003) ("Another barrier has been the transience of vendors; many early [electronic medical records (EMR)] developers are in precarious financial positions or event defunct. Consequently, primary care practices see implementing EMRs from current vendors as risky.").

232. *In Just One Year, the Number of EHR-Related Lawsuits Doubled*, ADVISORY BOARD (May 6, 2015, 8:41 AM), https://www.advisory.com/daily-briefing/2015/05/06/ehr-lawsuits [https://perma.cc/2PFC-RAU6] [hereinafter ADVISORY BOARD]; Lisa Schencker, *EHR Safety Goes to Court*, MOD. HEALTHCARE (June 25, 2016), http://www.modernhealthcare.com/article/20160625/MAGAZINE/306259982 [https://perma.cc/7LKR-S5EC].

233. ADVISORY BOARD, *supra* note 232.

234. *Id.*

Modern Healthcare, "Medical malpractice insurer the Doctors Co. closed twenty-eight claims in 2013 involving EHRs, and nearly that many during the first two quarters of 2014. In all, the Doctors Co. closed ninety-seven claims involving EHRs from January 2007 to June 2014."[235] To the extent that this trend continues to increase, litigation and legal costs could further stress the financial stability of the EHR market and many existing healthcare facilities.

Similar to those issues raised in a malpractice lawsuit, patient safety has also become a focus, particularly in a case involving a warring healthcare provider and an EHR vendor.[236] In this particular lawsuit, EHR-vendor Cerner filed a breach of contract lawsuit against PinnacleHealth after PinnacleHealth cancelled its twenty-year contract with Siemens (which was bought by Cerner) and instead entered into a contract with Siemen's competitor, Epic Systems Corp.[237] PinnacleHealth filed a counterclaim alleging fraud and breach of contract related to various patient safety issues that came about as a result of the Cerner EHR-software.[238] These patient safety issues included challenges in discharging a patient with the wrong medication, ordering pharmaceuticals not available to certain patients as a result of the EHR system, and failing to track patients.[239]

While malpractice and patient safety claims related to EHRs remain relatively low, there are nevertheless real concerns to the extent that these claims have become more widespread. First, individual user error accounts for the vast majority of the one percent of malpractice claims against vendors that have already been filed.[240] Additionally, even if a plaintiff could prove that the error was in fact inherent in the structure, design, or operation of the EHR system, providers are often still taking on the greatest level of risk because EHR vendors frequently include "hold harmless" provisions in their contracts that make it difficult for the provider to seek redress from the vendor.[241] Even if such claims are

235. Schencker, *supra* note 232.

236. *Id.*

237. *Id.*

238. Answer, Amended New Matter, Amended Counterclaim, Third-Party Complaint and Jury Demand, Cerner Health Servs., Inc. v. Pinnacle Health Sys., No. 15-05453 (C.P., Chester City, Pa. May 23, 2016).

239. *Id.* at 65–72.

240. Schencker, *supra* note 232 (noting that 64% of EHR-related claims in this sample involved user errors, 42% involved issues with the EHR system itself (some with more than one contributing factor), 10% involved a failure of system design, and 9% involved an electronic system or technology failure).

241. *Id.* Even with this increase in claims against EHRs, many critics argue that EHRs, nevertheless, make care better and generally improve patient safety as opposed to undermine it. *See also* ADVISORY BOARD, *supra* note 232.

challenging to prove, the fact that EHR vendors could face increased liability (and related costs) may create financial issues for certain EHR companies, which in turn will create difficulties for clients and customers in the form of increased costs, decreased financial stability of existing companies, and resulting transitions.

Despite government regulations to combat cyberattacks in the form of the CFAA and now the CISA, there are nevertheless distinct and significant challenges to addressing and combatting sophisticated cyberattacks, especially those affecting patient safety such as malware attacks. While the CFAA creates an enforcement mechanism for catching perpetrators of malware attacks and carries substantial penalties, jurisdictional challenges remain as many attacks occur in locations outside the United States, and hackers remain elusive with sophisticated methods of remaining relatively anonymous.[242] In contrast, the CISA is intended to share information among industry professionals to enable them to work together to prevent attacks from happening, but the voluntary nature of the program and necessary infrastructure development for the healthcare sector make it difficult for this law to be any sort of immediate response or solution to the recent cyberattacks.[243] Likewise, changes and shifts in the industry and some consolidation in the very crowded field of EHR space have contributed to some past market instability, and it seems as though this trend may continue over the next few years.[244] This lack of stability along with a trend toward increased liability for EHR vendors could hold the industry back from moving more rapidly away from focusing on EHR adoption and more toward promoting greater security in EHR products.

III. ADDRESSING AND COMBATING CYBER CONCERNS

While HIPAA and HITECH provide an existing structure for addressing security concerns and although certain updates and changes are certainly warranted for a now thirteen-year-old law, it would be naïve to think that simply updating the now-antiquated law can be the only sufficient solution. Rather, the approach must be multi-faceted and include not only some changes to existing law—including changes to HIPAA,

242. *See* Greenemeir, *supra* note 156.

243. *See generally supra* notes 211–217.

244. Ross Koppel & Christopher U. Lehmann, *Implications of an Emerging EHR Monoculture for Hospitals and Healthcare Systems*, 22 J. AM. MED. INFORMATICS ASS'N 465, 466 (Oct. 23, 2014) (noting that while there is some increased pressure for industry consolidation, existing vendor products compete greatly, and thus, integration will take years and pressure for competing data standards will be enhanced by consolidation).

HITECH and others—but also to the culture and demands of the healthcare industry. Any changes to existing law must also be accompanied by some shifts in the industry wherein healthcare providers not only move IT and IT security to the forefront of their priorities but also demand a better product from their EHR vendors.[245] Additionally, the industry must work on moving closer to HIPAA's ultimate goals of interoperability and communication between EHR systems to reduce some of the fragmentation that makes healthcare providers such an easy target. The following subsections will now address each of those proposed solutions in turn.

A. Amending HIPAA and Other Laws

Leaving existing regulations in their current form cannot be a solution, and it seems equally clear that while updating the now thirteen-year-old security regulations under HIPAA may help curb ransomware attacks and other cyberattacks, that cannot be the singular solution.[246] HIPAA, in its origins, was intended more for the purpose of improving healthcare outcomes and patient care by creating better communication and information exchange between providers and reducing some of the fragmentation that has plagued the U.S. healthcare system since the late 1970s.[247] With this focus in mind, the security concerns, which emerged in an age of a less sophisticated internet marketplace, first emphasized preventing public disclosures *by the provider* of a patient's private health information.[248] Thus, the regulations emphasized the actions of the healthcare entity, through its employees, agents, and business associates, as the most likely disclosing entity.

In contrast, ransomware and related attacks are rarely coming from authorized users within the HIPAA-covered entity; rather, such access is being sought by third parties attempting to access the data externally.[249]

---

245. *See* Kevin Lonergan, *Why the Healthcare Industry Badly Needs a Cyber Security Health Check*, INFO. AGE (Aug. 25, 2015), http://www.information-age.com/why-healthcare-industry-badly-needs-cyber-security-health-check-123460052/ [https://perma.cc/VJ4H-8J4P] ("Hospitals are often easier targets for cyber-crime because they lack proper cyber security defenses. Healthcare spending for cyber security is known to be low, compared to other regulated industries.").

246. *See generally supra* notes 66–67.

247. *See supra* notes 27–29.

248. Many of the early cases in which HIPAA was first utilized are cases that typically involved state law claims such as breach of confidentiality, breach of contract, or intentional infliction of emotional distress (as a result of information that was disclosed publicly, causing job loss or loss of family and friends due to stress or embarrassment). *See, e.g.*, Humphers v. First Interstate Bank of Or., 696 P.2d 527 (Or. 1985); Doe v. Medlantic Health Care Group, Inc., 814 A.2d 939 (2003).

249. *See Should HIPAA Be Expanded to Improve Defenses Against Hackers?*, HIPAA J. (Feb. 12, 2015), http://www.hipaajournal.com/hipaa-expanded-improve-defenses-hackers-017/

Granted, with the initial slow adoption of EHR systems, amending the security regulations sufficient to maintain pace with the rapid expansion and evolution of cybercrimes became secondary to simply encouraging use of EHRs and ensuring providers had time to adjust to the HIPAA disclosure regulations under the Privacy Rule.[250] Now that such EHR adoption has become more widespread,[251] more emphasis needs to be placed on making sure that the regulations enacted are actually addressing the current concerns of third parties.[252] While many healthcare providers are in the process of implementing "meaningful use" regulations and new quality reporting requirements required by various programs under the ACA,[253] hackers' new methods and approaches are expanding and evolving at a pace that, unfortunately, cannot provide healthcare providers with needed time to adjust to new changes.[254] Therefore, it is critical that such amendments have a more aggressive and expansive approach to addressing threats to security from outside, third-party attackers.

Fortunately, it is not necessary for HHS or lawmakers to develop amendments anew, as there are already various resources available to the industry to help providers enhance and expand their security protections.[255] Currently, such guidance is informational only and leaves the onus on healthcare providers (and perhaps, to some extent, EHR

[https://perma.cc/8TNM-F76D] [hereinafter HIPAA J.] (commenting that one issue with security regulation under HIPAA is a lack of requirement for data encryption, but noting that in many of the large scale breaches, the hacker(s) has been able to gain access to a system administrator's ID and password, which means that encryption would not have helped because the hacker would thus have access to encrypted files).

250. *See* Sittig & Singh, *supra* note 38.

251. *See* HENRY ET AL., *supra* note 32 (noting that more than 96% of hospitals have at least purchased a certified EHR).

252. There are still some critics who contend that the industry as a whole is still not entirely ready for any changes, because it is still attempting to implement the "meaningful use" regulations and adjust to life in an electronic world. *See* HIPAA J., *supra* note 249 ("Legislation updates are unlikely to bring about fast change in the healthcare industry as data privacy and security rules introduced in 2000 and 2003 are still not universally being followed. Instead of increased legislation, it is perhaps better to concentrate on enforcing the rules that have already been introduced.").

253. *See generally* James R. Horney & Paul N. Van de Water, *House-Passed and Senate Health Bills Reduce Deficit, Slow Health Care Costs, and Include Realistic Medicare Savings*, CTR. ON BUDGET & POL'Y PRIORITIES (Dec. 5, 2009), http://www.cbpp.org/research/house-passed-and-senate-health-bills-reduce-deficit-slow-health-care-costs-and-include [https://perma.cc/Q6TH-39EZ] (summarizing various cost control and quality measures under the ACA).

254. *See* Zetter II, *supra* note 105.

255. *See* CROSSWALK, *supra* note 24, at 1–2 (noting that those who implement best practices under the guidelines "should not assume that by so doing they are in full compliance with the Security Rule"); U.S. FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Dec. 28, 2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf [hereinafter FDA POSTMARKET MANAGEMENT GUIDANCE].

vendors) to impose on themselves measures and methods more exacting than legally required.[256] HHS has worked with the NIST to create a HIPAA crosswalk to NIST's Cybersecurity Framework and through the Food and Drug Administration (FDA) to issue guidance on cybersecurity for medical devices.[257] HHS likewise reiterated in its Fact Sheet that, while the HIPAA privacy and security rules help provide a base for addressing cybersecurity concerns, HHS encourages providers to undertake their own protections above and beyond those required.[258] These documents provide advice and information to providers on best practices for cybersecurity—these practices, at times, make recommendations beyond HIPAA compliance, thus exposing to providers areas in which they may remain vulnerable.[259] Each of the publications cross-references one another and recommend the others as alternative sources that could be helpful for developing a comprehensive cybersecurity program.[260] Consistent with recent efforts set forth under the CISA, the FDA and NIST guidance recommends participation in some sort of sharing forum in order to exchange information with other providers about existing threats.[261] While these resources are helpful—as are several other resources available through HHS, such as the HHS Security Risk Assessment Tool[262]—the current approach requires providers to consult various resources and puts

256. *See* FDA POSTMARKET MANAGEMENT GUIDANCE, *supra* note 254, at 8. *See generally Ransomware Fact Sheet*, *supra* note 81.

257. *See* FDA POSTMARKET MANAGEMENT GUIDANCE, *supra* note 255, at 4–5.

258. *See Ransomware Fact Sheet*, *supra* note 81, at 2.

259. One of the most common entry points for hackers is through medical devices that are not, as a singular device, subject to the HIPAA regulations, but which carry PHI and connect to a larger hospital or health system network through the interconnectivity of the devices to the system. For an extensive discussion on how specifically to address the risks of medical devices to cybersecurity generally, see generally Wellington, *supra* note 144.

260. CROSSWALK, *supra* note 24, at 2; FDA POSTMARKET MANAGEMENT GUIDANCE, *supra* note 255, at 6–7.

261. CROSSWALK, *supra* note 24, at 8 (stating that the HIPAA Security Rule does not have a provision that corresponds to NIST's framework requirement that "[t]hreat and vulnerability information is received from information sharing forums and sources," but noting in a footnote that the HIPAA Security Rule does require a breach analysis and therefore there is some reporting of information to the extent a breach is identified and some of this information is thus shared publicly); *see also* FDA POSTMARKET MANAGEMENT GUIDANCE, *supra* note 255, at 6 ("Critical to the adoption of proactive, rather than reactive, postmarket cybersecurity approach is the sharing of cyber risk information and intelligence within the medical device community. This information sharing can enhance management of individual cybersecurity vulnerabilities and provide advance cyber threat information to additional relevant stakeholders to manage and enhance cybersecurity in the medical device community and HPH Sector.").

262. *See Security Risk Assessment*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/security-risk-assessment [https://perma.cc/XP2D-2AZM] (tool available for download from this site).

the onus on the provider to decide which of the recommendations it should implement beyond HIPAA-compliance measures.[263]

While such voluntary options may be helpful for purposes of not overwhelming or overloading those in the healthcare industry with additional new obligations when it comes to cybersecurity, it is not particularly helpful in impressing upon the industry the true necessity for compliance with known risks.[264] It also leaves HIPAA-covered entities, especially those that are already struggling to make—under meaningful use requirements—costly investments in EHR systems, with having to prioritize which security regulations beyond HIPAA may be helpful, beneficial, or even necessary for ensuring appropriate protection of data. Incorporating other guidance into the HIPAA Security Rule—including incorporation of medical devices, data stored and exchanged on medical devices, and encryption of data—will provide clarity for HIPAA-covered entities and will ensure that EHR products on the market incorporate greater security provisions in order to be able to certify the product as HIPAA-compliant.[265]

Although the CISA has many critics, it seems that the bill is at least a step in the right direction toward developing a more comprehensive approach from the healthcare community about how to address these risks and how to safely share such data within the confines of HIPAA.[266] It is perhaps true that, in this world of rapidly changing and advancing technology and cyber threats, the healthcare industry does not have the luxury to wait a year for recommendations, especially in a reporting structure that is retrospective in nature.[267] Additionally, without any obligation to report, it is not clear whether, even with recommendations, the CISA will have achieved its intended benefit.[268] It is necessary, however, to begin somewhere and, prior to making any information sharing mandatory on healthcare providers, it seems advisable to explore appropriate processes and determine best practices for how and in what manner this data can safely be shared without compromising patient privacy concerns. It will be vital for HHS to act quickly once the task force has completed its work to implement any recommendations, including

263. *HIPAA Security Rule*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/healthcare/security/hipaa-security-rule [https://perma.cc/6SK6-K9ZG] ("In the preamble to the Security Rule, several NIST publications were cited as potentially valuable resources for readers with specific questions and concerns about IT security.").

264. *See* Zetter II, *supra* note 105.

265. *See* Snell, *supra* note 67.

266. One such step might first be the acknowledgement that sharing of healthcare data is unique and different than other data and thus necessitates a healthcare task force that might adopt a different approach to data sharing. *See generally* 6 U.S.C. § 1533 (2015).

267. *See* Frank, *supra* note 218.

268. *See* Rosenfeld, *supra* note 171.

promulgation of regulations as needed, if certain changes are deemed necessary, in order to assure cybersecurity in the healthcare arena.

B. Changes to Industry Operations and Culture

Even if certain legislative changes are made, changes to industry operations and culture are still needed to fully address the cybersecurity threats that are affecting the healthcare industry. As has been demonstrated by the slow adoption of EHRs following HIPAA and the continued challenges healthcare companies are encountering in trying to implement HITECH and "meaningful use" regulations,[269] the healthcare industry has not arrived at its transition to an electronic system organically or in response to patient demand.[270] Rather, many healthcare providers have adopted the use of electronic medical records reluctantly and with great trepidation, mostly driven by concerns about the expense and the impact that such use will have on practice and productivity.[271] As a result, adoption and implementation of regulations has been challenging, in spite of regulations being in place since 2003.[272]

The emergence and use of technology in healthcare stands in stark contrast to that of the banking industry, and this might give some clues as to why cybersecurity is so much more pronounced and established in the banking industry.[273] "Electronic banking"[274] first rose to popularity in the

---

269. *See* Sittig & Singh, *supra* note 38.

270. *Id.*

271. *See* Dawn Heisey-Grove et al., *A National Study of Challenges to Electronic Health Record Adoption and Meaningful Use*, 52 MED. CARE 144, 146–47 (Feb. 2014), http://journals.lww.com/lww-medicalcare/Documents/13-00342.pdf. Regarding implementation of meaningful use regulations and associated challenges, the report noted: "Providers in small private practices require assistance along all steps of the [Security Risk Analysis ("SRA")] process, as they usually do not have in-house, IT, vendor or privacy and security expertise. Practice staff typically need education and training on privacy and security compliance, how to perform the SRA, and how to implement mitigation of issues identified in the SRA." *Id.* at 147.

272. *Id.* at 144; Brian Schilling, *The Federal Government Has Put Billions Into Promoting Electronic Health Record Use: How Is It Going?*, COMMONWEALTH FUND, QUALITY MATTERS ARCHIVE, June/July 2011, http://www.commonwealthfund.org/publications/newsletters/quality-matters/2011/june-july-2011/in-focus [https://perma.cc/CT32-D6GK].

273. Beth Kutscher, *Healthcare Underspends on Cybersecurity as Attacks Accelerate*, MOD. HEALTHCARE (Mar. 3, 2016), http://www.modernhealthcare.com/article/20160303/NEWS/160309922 [https://perma.cc/E6ZW-RH8V] (contrasting spending by healthcare providers on cybersecurity at less than six percent of budget to financial and banking institutions that spend twelve to fifteen percent).

274. Technically, there are different forms of electronic banking, including online banking (customers being able to access their account information online, including features like online bill pay and transferring of funds between accounts, and through software connected between a personal computer and the bank's server), web-based banking (the same concept as online banking, but through a web-portal through the bank's central computers), and internet banks, which are banks that only exist in an electronic world and do not have a physical brick and mortar location. *See* Kimbrelly Kegler,

late 1990s when both brick-and-mortar banks[275] and new internet-only banks began offering the same services via the internet.[276] Much of this evolution arose out of consumer demand for banking services that were more accessible and user friendly and did not require trips to the bank during banking-only hours.[277] Thus, in order to compete with the introduction of a new competitor—the internet-only bank—brick-and-mortar banks had to adapt and provide competing services to their customers, some of which have involved incentives for the consumer to use online resources as opposed to paper transactions.[278]

Once banks began utilizing these online services, they realized the financial savings that would come along with such shifts to an online system, which motivated both consumers and banks to make the shift to an online platform.[279] Thus, the move toward electronic banking was consumer driven, but banks (both brick-and-mortar and internet-only) soon realized the value of online banking from a cost perspective, and they were also motivated to continue and expand the practice.[280]

Once the industry was inspired to move consumers to an online platform, there was equal incentive to ensure that there was sufficient security and privacy, not simply for compliance with the Electronic Funds Transfer Act (EFTA),[281] the Right to Financial Privacy Act,[282] and the Fair Credit Reporting Act,[283] but because consumers who did not feel their

---

Electronic Banking: Security, Privacy, and CRA Compliance, 2 N.C. BANKING INST. 426, 428–33 (1998).

275. "Brick-and-mortar" is defined as "relating to or being a traditional business serving customers in a building as contrasted to an online business." MERRIAM-WEBSTER DICTIONARY.

276. *See* Christian N. Watson, *The Growth of Internet-Only Banks: Brick and Mortar Branches are Feeling the "Byte,"* 4 N.C. BANKING INST. 345, 346–47 (2000) (describing the distinctions between the use by traditional banks of online services and also the emergence of Internet-only banks in which there is no physical building or branch, but rather just an online presence).

277. *Id.* at 346 ("Customer demand for access to their bank accounts via the Web led to the creation of the second type of electronic banking, the true Internet-only bank.").

278. *Id.* at 346–48. Part of this push by banks to move individuals to an online banking platform is because of the reduced cost of this type of service. As noted by Christian Watson, "The new Internet banks have obvious advantages, such as no branch maintenance, fewer personnel costs, no paper, and no time and place limitations. . . . Banking via the Internet is markedly cheaper than using other channels." *Id.* at 349.

279. *Id.* at 349.

280. *Id.* at 351–52.

281. 15 U.S.C. §§ 1693–1693r (2012); 12 C.F.R. § 205.6(b) (2001) (Electronic Fund Transfers (Regulation E)). The EFTA sets forth rights and responsibilities of parties to an electronic funds transfer with a focus on consumer protection, including provisions regarding release of information to a third party regarding the consumer's account. 15 U.S.C. § 1693c (2012).

282. 12 U.S.C. §§ 3401–3422 (2012). This law prevents financial institutions from disclosing an individual's financial information without an authorization, judicial summons, or search warrant.

283. 15 U.S.C. § 1681–1681x (2012). This law prevents institutions from disclosing consumer report information (which contains financial data) other than under specific circumstances. All three

information would be secure online would be less inclined to participate.[284] Therefore, the banking industry developed industry standards and methods for addressing hackers and other cyber risks in large part to ensure consumers would have faith and trust in an online banking system and would continue to use it.[285]

The healthcare market, however, makes it difficult to assume that EHRs would have a similar trajectory to the banking industry. For example, unlike the banking industry, the healthcare industry has no clear "consumer" to drive a similar movement.[286] Patients certainly stand to benefit from the use of EHRs through an ability to have greater interaction with their provider through email or online portals, greater access to health information, and less likelihood of duplicative services. But, the entities that pay for the bulk of those services—insurers and the federal government through its operation of federal healthcare programs—also stand to gain through use of EHRs, but for different and perhaps sometimes opposing reasons to patients.[287] Regarding individual patients, a study conducted in 2009 concluded that

> [w]hile only 9 percent of consumers surveyed have an electronic personal health record [(PHR)], 42 percent are interested in establishing PHRs connected online to their physicians. Fifty-five percent want the ability to communicate with their doctor via e-mail to exchange health information and get answers to questions. Fifty-seven percent reported they'd be interested in scheduling

---

of these laws predated development of the Internet or online banking, so, unlike HIPAA, they were drafted in response to security and privacy concerns in a paper world.

284. Kegler, *supra* 274, at 437.

285. This was especially critical for Internet-only banks, which relied entirely on consumer trust of the bank to maintain security and privacy of their financial information in cyberspace.

286. *See* Bates, *supra* note 231, at 2 (noting that the federal government, as the largest purchaser of American health care, should lead the way toward adoption of electronic medical records by healthcare providers).

287. FURROW, *supra* note 28, at 11 ("[A]gency relationships, which pervade health markets, are highly influential in health care transactions. Most people 'purchase' health care services with the assistance of multiple agents—their employers, the plans or insurers chosen by their employers, and, significantly, the physicians who guide their choices."); *see also id.* at 631 ("In understanding the structure of health insurance, the crucial relationship is between those who deliver medical care and those who pay for it. Even a passive indemnity insurer stands between the patient and the medical provider, as a financial intermediary and an underwriter of risk. Today, with risk shifting from insurers to employers, and with financial intermediaries playing more of an administrative role than in the past, the trilateral relationship is more complex.").

> appointments, buying prescriptions and completing other transactions online if their information is protected.[288]

Insurers and the federal government, on the other hand, are more concerned about the benefits for greater efficiency and patient safety, such as "decision support regarding the cost and selection of drugs, laboratory tests, and radiographic studies,"[289] and reminders and prevention guidelines for better management of chronic conditions, all of which should result in lower overall costs for health services.[290] There are multiple consumers and multiple decision makers in the healthcare industry having differing needs and desires in terms of the benefits of an EHR. This distinctive demand does not supply providers with a clear "product" or necessary functions for implementation and development of an EHR system.

Because of this challenge of identifying and defining the consumer to whom the healthcare industry is catering, the push toward EHRs came not from consumer demand and a recognized cost savings, such as in the banking industry, but rather from federal regulations.[291] Recognizing complications and flaws in the U.S. healthcare system,[292] policy experts (who then advised U.S. Congress) first promoted the idea that improving the healthcare system would require a "major federal investment in information technology" because such technology was "essential to provide better care at lower cost."[293] Thus, unlike banking, EHRs arose

---

288. Bernie Monegain, *Consumer Demand for Healthcare IT 'Never Stronger,' Survey Shows*, HEALTHCARE IT NEWS (Apr. 14, 2009, 10:06 AM), http://www.healthcareitnews.com/news/consumer-demand-healthcare-it-never-stronger-survey-shows [https://perma.cc/VJX3-R79Z].

289. Bates, *supra* note 231, at 4.

290. *See id.*

291. *See* FURROW, *supra* note 28.

292. Around the time of enactment of HIPAA and during promulgation of its regulations, there were a number of influential studies that came out highlighting that the expense of the U.S. healthcare system did not necessarily equate to its effectiveness or outcomes. A 1999 report from the World Health Organization (WHO) ranked the U.S.' healthcare system 37th among other developed countries. Bates, *supra* note 231, at 2 (citing G.F. Anderson & J.P. Poullier, *Health Spending, Access, and Outcomes: Trends in Industrialized Countries*, HEALTH AFFAIRS (May 1999)). Likewise, the Institute of Medicine issued a report in 2001 titled, *Crossing the Quality Chasm*, that referred to the U.S. healthcare system as fundamentally broken. *Id.* (citing COMMITTEE ON QUALITY OF HEALTH CARE IN AMERICA, INST. OF MED., CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY (2001)). While there were some early adopters of EHRs prior to implementation of HIPAA, much of the healthcare industry struggled to adopt EHRs for a variety of reasons including high cost, organizational capabilities, etc. *See generally* Samuel J. Wang et al., *A Cost–Benefit Analysis of Electronic Medical Records in Primary Care*, 114 AM. J. MED. 397 (2003); AGENCY FOR HEALTHCARE RES. & QUALITY, *Electronic Medical Record Systems*, https://healthit.ahrq.gov/key-topics/electronic-medical-record-systems [https://perma.cc/2QYZ-ZBUC]; sources cited *supra* notes 26–35.

293. Bates, *supra* note 231, at 2.

not out of *competitive* necessity but out of *legal* necessity, and therefore, the accompanying security and privacy approaches were adopted not to ensure that consumers would continue to use one's product but merely to comply with applicable laws.[294] This culture has permeated the slow adoption of EHR use and the lack of willingness to make substantial investments in health information technology.[295]

With the use of technology being led through federal regulations, the consequences likewise are legislative in nature, such as the assessment of fines and penalties and required public reporting.[296] But, unlike the relatively small fines and penalties that have been levied against providers for HIPAA violations in the past, ransomware attacks appear to be a possible catalyst for finally creating a cultural shift in the healthcare marketplace that will stress the importance of cybersecurity. Notwithstanding the bitcoin ransom demand, hospitals and other health systems that experience ransomware attacks suffer genuine financial consequences.[297] As mentioned in the Introduction, the Baltimore-based MedStar system was forced to cancel many appointments at its outpatient facilities, and its primary hospital was eventually unable to triage patients sufficiently, such that it was forced to go on diversion for new patients arriving in the emergency room.[298] The financial consequences of this type of attack are potentially substantial for a large system like MedStar,[299] but could be even more devastating for a smaller system or singular hospital that may not have financial capital to withstand this type of attack.[300]

---

294. *See* Kutscher, *supra* note 273.

295. *See id.*; Yaraghi, *supra* note 55.

296. *See generally* 45 C.F.R. § 160 (2013).

297. John Woodrow Cox, *Possible 'Ransomware' Attack Still Crippling Some MedStar Hospitals' Computers*, WASH. POST (Mar. 30, 2016), https://www.washingtonpost.com/local/likely-ransomware-cyberattack-still-crippling-medstar-health-computers-at-some-hospitals/2016/03/30/a82c9fa8-f687-11e5-8b23-538270a1ca31_story.html?utm_term=.a28e738225d3 [https://perma.cc/W5HH-DTQR] (noting that FBI agents investigated 2,453 complaints regarding ransomware attacks in 2015, costing the target entities an estimated $24.1 million).

298. *See* Cox, *supra* note 2.

299. *See* Dennis Foley, *MedStar IT System Mostly Back to Full Operation After Cyber Attack*, WTOP (Apr. 4, 2016, 12:38 PM), http://wtop.com/local/2016/04/medstar-says-system-mostly-back-full-operation/ [https://perma.cc/J2UV-5KE6] (noting that MedStar officials stated that they had not looked at the financial impact of the attack as of yet).

300. For analysis of potential costs beyond ransomware demand (if paid), see Christiaan Beek, *Healthcare Organizations Must Consider the Financial Impact of Ransomware Attacks*, DARKREADING (Apr. 7, 2016, 2:52 PM), http://www.darkreading.com/partner-perspectives/intel/healthcare-organizations-must-consider-the-financial-impact-of-ransomware-attacks/a/d-id/1325030 [https://perma.cc/A92V-9RSU] (noting that healthcare organizations have to consider costs of lost or stolen records, downtime costs (including delays in surgeries, appointments, lab results, etc.), and incident response and audit/assessment services).

According to a study by the Ponemon Institute, the potential cost of a data breach is about $355 per patient record.[301] The same study noted that 45% of all breaches in the study were the result of a malicious or criminal attack.[302] What are not included in this number or in current calculations are the potential litigation costs that may result from patient safety incidents.[303] To the extent that a hospital or health system is hit with a ransomware attack and such attack results in an issue affecting patient safety, such as delayed care, medication errors, surgical delays, etc., it is possible that patients who are harmed by such errors could file medical malpractice claims.[304] Perhaps with the increased financial and reputational risks posed by ransomware attacks, the healthcare industry will receive a much needed nudge toward a cultural shift that begins to focus on the necessity for cybersecurity. Without this cultural shift pursuant to which the industry as a whole takes steps toward adopting a greater emphasis on cybersecurity, it is unlikely that changes in the law will bring about the necessary modifications.

In order for this movement to take hold, it is necessary for the healthcare industry to move toward creating its own best practices regarding cybersecurity. Perhaps the task force formed under the CISA will be helpful in implementing this process, but the healthcare industry can ill afford to delay taking necessary steps much longer, as hackers and ransomware attackers are developing more and more sophisticated tools and methods.[305] Unlike the slow march to adoption and use of EHRs, which waited for government regulators to impose restrictions and set standards, providers and insurers instead must move toward implementation of these best practices through self-regulation and lead the way for government regulators. Like the banking industry, players in the healthcare industry must take a proactive step toward assuring cybersecurity not because regulations require them to do so, but because the consequences of waiting on regulations to catch up could be potentially devastating to patients and also the financial well-being of the institutions themselves.[306]

Once healthcare providers and other purchasers of EHR systems begin to demand more from their EHR system than simply HIPAA compliance, two consequences may affect the EHR vendor market. First, to the extent that hospitals and health systems, as consumers and

301. PONEMON INSTITUTE, 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2 (2016), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN.

302. *Id.* at 11.

303. *See* ADVISORY BOARD, *supra* note 232.

304. *Id.*

305. *See* FBI, *supra* note 107; Zetter II, *supra* note 105.

306. *See* Kegler, *supra* note 274.

purchasers, demand more sophisticated and advanced cybersecurity in their EHR products—beyond simple compliance with the law—the vendors will have to provide such enhancements in order to compete in the market. Second, it is possible that current market consolidation will continue, as only EHR companies that have sufficient capabilities and financial resources to add these enhancements will be able to compete in the marketplace.[307] As more consolidation occurs, and hopefully more interoperability among vendors as is intended to be the eventual result of HIPAA and HITECH, there can be more information gathering and sharing about the types and kinds of attacks that are happening and how such attacks can be prevented. To the extent that there are fewer vendors in the market and more vendors are able to communicate with one another in a HIPAA-compliant fashion, many of the concerns raised regarding security and privacy in connection with the CISA will be eliminated.[308] Consolidation will not eliminate ransomware attacks, but it will increase the capabilities of the EHR vendors to be aware of the type of attacks that are occurring and what steps or methods have been employed effectively in order to eliminate or reduce such attacks.

CONCLUSION

As Ryan Witt, vice president and managing director of the healthcare industry practice at Fortinet,[309] stated, "Ransomware will get worse before it gets better . . . . You don't want to think of return on investment as it pertains to criminal activity, but there is a strong [return on investment], and these attackers are quite sophisticated and know there is money to be made."[310] Hospitals and health systems are especially vulnerable to these types of attacks not only because of the critical nature of the services that hospitals provide, making their inability to function potentially more devastating, but because of a lack of updated laws that provide sufficient protection against the cyberattacks and a cultural attitude that has thus far failed to fully embrace the need for substantial and ongoing investments in healthcare information technology.[311]

---

307. *See* Bates, *supra* note 231, at 6.

308. *See* Joseph Conn, *Healthcare Industry Giants Pledge to Ease Interoperability, EHR Use*, MOD. HEALTHCARE (Feb. 29, 2016), http://www.modernhealthcare.com/article/20160229/NEWS/160229866 [https://perma.cc/Q7XY-QA38].

309. Fortinet is a company that provides network and content security for various institutions, including the healthcare industry. *See About Us*, FORTINET, https://www.fortinet.com/corporate/about-us/about-us.html [https://perma.cc/Z6R3-DXK9].

310. Bill Siwicki, *Ransomware Attackers Collect Ransom from Kansas Hospital, Don't Unlock all the Data, then Demand More Money*, HEALTHCARE IT NEWS (May 23, 2016, 2:58 PM), http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom [https://perma.cc/K8GG-99T8].

311. *See* Kutscher, *supra* note 273.

To the extent that hospitals and health systems are going to survive and potentially thwart these attacks, not only do regulators need to update and amend existing laws to bring them up to date with current technology by incorporating protections that might help guard against these attacks, but the healthcare industry as a whole needs to shift its focus to create greater emphasis and energy around the importance of cybersecurity. Industry leaders need to develop best practices that supply providers and other healthcare industry participants with necessary tools not just to comply with laws but also to help actually prevent such attacks. This can be accomplished in part by also demanding better and more sophisticated products that incorporate more up-to-date cybersecurity provisions from EHR vendors. This will not necessarily be easy for healthcare providers, as it will require more capital investment for software updates and patches and better control over medical devices and how such devices interact with the hospital's larger EHR.[312] To the extent that providers become more demanding and expectant of their EHR products, this could lead to EHR vendor consolidation, which may in turn enable easier and safer sharing of necessary data regarding cyberattacks to help combat issues on a more prospective as opposed to retrospective basis.

While ensuring that there are sufficient laws in place to protect patients and their personal health information is vital; it is simply not enough to believe that the healthcare industry can approach these latest attacks in the same way that they have approached EHR adoption generally. Hospitals and health systems should heed the advice of cybersecurity specialists such as Ed Cabrera, vice president for cybersecurity strategy at Trend Micro, "If these attacks make hospitals take a hard look at their security and take these threats seriously, in the end it could be a good thing. . . . This is a risk they can't ignore anymore."[313]

312. *See* Wellington, *supra* note 144, at 145–48.

313. Keith Wagstaff, *Big Paydays Force Hospitals to Prepare for Ransomware Attacks*, NBC NEWS (Apr. 23, 2016, 6:06 AM), http://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176 [https://perma.cc/7ZTW-G6LV].