Indiana Health Law Review

Volume XV **2018** **Number 2**

NOTE

ONCE MORE UNTO THE BREACH: HOW THE GROWING THREAT OF RANSOMWARE AFFECTS HIPAA COMPLIANCE FOR COVERED ENTITIES

CONNOR MCLARREN*

I. INTRODUCTION

Imagine you run one of the largest hospital systems on the East Coast, serving hundreds of thousands of patients on a yearly basis and providing critical healthcare-related services. Your electronic health records, those of every patient you have ever seen, are critical for ensuring proper medical care, treatment, payment, and are necessary for the proper day-to-day functioning of your enterprise on every imaginable level. Now imagine that one day, access to your entire computer system is taken away, and put in the hands of unknown hackers. All they leave you is a ransom notice: either pay the equivalent of tens of thousands of dollars in "Bitcoin," or lose your access to this critical data forever.

This is the exact experience of the Medstar hospital system in the greater Washington D.C. area, a five-billion dollar health-care provider with ten hospitals, 250 outpatient centers, and over 30,000 employees.[1] For days, its entire system was overtaken by a dangerous and increasingly more common threat to the healthcare infrastructure of the United States: ransomware.[2]

A. The Issue: Ransomware Challenges Traditional Notions of HIPAA Breaches

As the healthcare industry has increasingly turned to digital records to store patients' health records, traditional legislation such as the Health Insurance Portability and Accountability Act (HIPAA) that have aimed at setting standards of security for protected health information (PHI) have proven incapable of keeping up with novel or unexpected vulnerabilities in the cybersecurity of

---

* J.D. Candidate, 2018, Indiana University McKinney School of Law; B.S., 2015, Samford University

1. John Woodrow Cox et. al., *Virus infects MedStar Health system's computers, forcing an online shutdown*, WASH. POST (Mar. 28, 2016), https://www.washingtonpost.com/local/virus-infects-medstar-health-systems-computers-hospital-officials-say/2016/03/28/480f7d66-f515-11e5-a3ce-f06b5ba21f33_story.html [https://perma.cc/6RUU-FJPT].

2. *Id.*

healthcare organizations.[3] Nowhere is this more evident than in the case of "ransomware" attacks. Ransomware is malware that is designed to lock hospitals out of their patient records while the responsible party issues a ransom to the hospital with a simple ultimatum: pay up or permanently lose access to all of its patient information.[4] The Department of Health and Human Services (HHS) defines ransomware as follows:

> [Ransomware is] a type of malware (malicious software) distinct from other malware; its defining characteristic is 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. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.[5]

The healthcare industry is now the most common target of ransomware attacks; reports suggest that hospitals were on the receiving end of 88% of all ransomware attacks.[6] While ransomware attacks are devastating to hospitals, they have also created a legal quandary: while the malware locks hospitals out of their access to patient health records, determining whether or not that data has actually been breached and accessed by a third-party can be difficult to determine and depends on the variant of ransomware used in the attack.[7] Thus far, over a million unique variants of ransomware have been discovered.[8]

B. Health and Human Services Reaction to Ransomware Attacks

In July of 2016, the HHS Office of Civil Rights (OCR) announced that "unless the [healthcare provider] or business associate can demonstrate that there is a '…low probability that the PHI has been compromised,' based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred."[9] In order to demonstrate that there was a low probability of a breach,

---

3. Jonathan Litchman, *The False Promise of HIPAA for Healthcare Cybersecurity*, HEALTH IT SECURITY (March 8, 2016), http://healthitsecurity.com/news/the-false-promise-of-hipaa-for-healthcare-cybersecurity [http://perma.cc/J4GX-96E5].

4. U.S. DEP'T. OF HEALTH & HUMAN SERVS., FACT SHEET: RANSOMWARE AND HIPAA (2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf [http://perma.cc/AS48-JNRP].

5. *Id.*

6. Max Green, *Hospitals are hit with 88% of all ransomware attacks*, HEALTH IT & CIO REV. (July 27, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html [http://perma.cc/E5JP-HLWF].

7. Matthew Mellen, *How to interpret HHS guidance on ransomware as a HIPAA breach*, HEALTH DATA MGMT. (July 27, 2016, 3:50 PM), http://www.healthdatamanagement.com/opinion/how-to-interpret-hhs-guidance-on-ransomware-as-a-hipaa-breach [http://perma.cc/H2JS-D67Q].

8. *Id.*

9. U.S. DEP'T. OF HEALTH & HUMAN SERVS., *supra* note 4.

a hospital must prove the following four factors, as laid out within the Breach Notification Rule:

(1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(2) the unauthorized person who used the PHI or to whom the disclosure was made;
(3) whether the PHI was actually acquired or viewed; and
(4) the extent to which the risk to the PHI has been mitigated.[10]

These criteria are problematic for several reasons. First, the criteria used to determine whether or not there was a low probability of a breach is highly fact-specific,[11] and might provide incentive to hospitals not to report a ransomware attack. Second, there is no guarantee that total compliance with HIPAA guidelines can prevent a breach from occurring,[12] and third, even encrypted data can be considered unencrypted by HHS if the ransomware attack also manages to overwrite the electronic protected health information ("ePHI") with its own encryption.[13]

This Note will set out to accomplish three primary goals. First, I will conduct an analysis of what ransomware is, along with other cybersecurity threats facing the healthcare industry today, as well as the steps that are being taken to counter the threat of ransomware in both the private and public sectors. Second, I will argue that current legislation and rulings regarding ransomware are inadequate in this matter based on current cybersecurity trends. Finally, I will provide two possible alternative routes with which the damage caused by ransomware could be mitigated.

I. BACKGROUND & HISTORY

A. Major Cybersecurity Attacks Within the Healthcare Industry

As more and more health records have been made electronic,[14] they have

---

10. *Id.*

11. *Id.*

12. Dennis Fisher, *HHS Issues Vague Guidance on Ransomware and HIPAA Disclosures*, ON THE WIRE (July 21, 2016), https://www.onthewire.io/hhs-issues-vague-guidance-on-ransomware-and-hipaa-disclosures/ [http://perma.cc/RS5L-PJZY].

13. Amy Gordon et. al., *Guidance on Ransomware Attacks under HIPAA and State Data Breach Notification Laws*, NATIONAL LAW REVIEW (Aug. 8, 2016), http://www.natlawreview.com/article/guidance-ransomware-attacks-under-hipaa-and-state-data-breach-notification-laws [http://perma.cc/4V6U-LLZF].

14. *Office-based Physician Electronic Health Record Adoption*, OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH. (Dec. 2016), https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php [http://perma.cc/65XS-TSD4] (outlining that the adoption of electronic medical records by doctors within the United States has more than doubled since 2008, from 42% to 87% by the end of 2016).

become increasingly exposed to threats from hackers. The first health-care related breaches were reported in 2005, but in 2009 attackers managed to collect over four million health records.[15] "Between 2012 and 2014, cybercriminals started to ramp up attacks on the healthcare industry, which remarkably suffered more than the business, military, and government sectors. In fact, the number of health care service provider victims has grown almost fourfold in 2014 from when it was first observed in 2005."[16] As time has gone on, attacks have become increasingly sophisticated, to the point that physical contact with hospital computer systems is no longer necessary or even required for a successful cyberattack.[17] Hackers can now use a combination of more traditional methods such as phishing scams over email, and far more unorthodox and innovative approaches such as making cyberattacks through unprotected medical devices.[18]

B. Why Are Covered Entities Such Prime Targets For Ransomware?

Hospitals have become a popular target because their cybersecurity is generally not as good as other industries and because hospitals require patient data records in order to properly function.[19] Electronic health records can be sold online for $10 to $50 each, making them an easy and profitable target for hackers to focus on.[20] Hospitals are easy prey, as the primary focus of hospitals – when it comes to digitalization – is HIPAA compliance rather than cybersecurity.[21] "You can't just roll out new software," explains Josephine Wolff, a computing security expert at the Rochester Institute of Technology, on why implementing new cybersecurity procedures can be so difficult for covered entities.[22] "The medical world is dealing with a very complicated legal and policy regime around medical data and how it has to be handled."[23]

---

15. *Medical Data in the Crosshairs: Why is Healthcare an Ideal Target?*, TREND MICRO (Aug. 14, 2015), http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/medical-data-in-the-crosshairs-why-is-healthcare-an-ideal-target [http://perma.cc/B36G-MQHH].

16. *Id.*

17. *Id.*

18. Kelly J. Higgins, *Hospital Medical Devices Used As Weapons In Cyberattacks*, DARK READING (June 8, 2015, 4:00 PM), http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751 [http://perma.cc/9BRN-BQ6A].

19. Annie Sneed, *The Most Vulnerable Ransomware Targets Are the Institutions We Rely On Most*, SCI. AM. (Mar. 23, 2016), https://www.scientificamerican.com/article/the-most-vulnerable-ransomware-targets-are-the-institutions-we-rely-on-most/ [https://perma.cc/AL7V-DCYA].

20. Nate Berg, *Hackers have figured out how easy it is to take down a hospital*, SPLINTER (Mar. 10, 2016, 4:17 PM), http://splinternews.com/hackers-have-figured-out-how-easy-it-is-to-take-down-a-1793855277 [https://perma.cc/CUU5-8SKJ].

21. 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/FX2E-DYV5].

22. Sneed, *supra* note 19.

23. *Id.*

Ransomware is not only a threat to administrative functions: the Department of Homeland Security (DHS) has issued statements of concern regarding the vulnerability of medical devices to ransomware attacks.[24] As Marty Edwards, director of DHS's Industrial Control Systems Cyber Emergency Response Team, succinctly summed up the threat, "It's only a matter of time before we see some sort of significant type of events that involve patient safety that are cyber enabled[.]"[25] He further noted that 2017 could see the first of such ransomware attacks against patient medical devices.[26] Further complicating this matter is a shortage of security professionals that hospital systems and other covered entities can reliably call upon for assistance.[27]

C. HIPAA and Cybersecurity

HIPAA has been around since the 1990's and has formed the foundation for protected health records, but only recently has Congress acted to reinforce the security of electronic health records. HIPAA, of course, governs the usage of PHI by covered entities: these entities can range from traditional medical practitioners and providers to medical billing-houses and including, most recently, business associates of healthcare providers who interact with PHI.[28] Essentially, if you interact with identifiable PHI, you are a covered entity.[29] In 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act, which, in addition to encouraging the adoption of electronic health records and other health information technology, also lays out privacy rules for how to protect electronic PHI.[30] HITECH requires that technologies and policies must comply with HIPAA privacy and security laws.[31] Most notably, the

---

24. Greg Slabodkin, *Ransomware emerging as medical device cybersecurity threat*, HEALTH DATA MGMT. (Feb. 20, 2017, 6:50 AM EST), http://www.healthdatamanagement.com/news/ransomware-emerging-as-medical-device-cybersecurity-threat [https://perma.cc/4XDQ-JQD7].

25. *Id.*

26. *Id.*

27. Andrea Peterson, *Why hackers are going after health-care providers*, THE WASHINGTON POST (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/4YAK-N5QZ].

28. *HIPAA 'Protected Health Information': What Does PHI Include?*, HIPAA.COM (Sept. 1, 2009), https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/ [https://perma.cc/WYX4-SZ6A]; *see also Business Associates*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/FAU6-FRXP] (last updated July 26, 2013).

29. *Id.*

30. *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T. OF HEALTH & HUMAN SERVS. (June 16, 2017), http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/ [https://perma.cc/ZN5F-ASD9].

31. Margaret Rouse, *HITECH Act (Health Information Technology for Economic and Clinical Health Act)*, TECHTARGET, http://searchhealthit.techtarget.com/definition/HITECH-Act

HITECH Act requires that any data breach suffered by a covered entity or business associate that affects 500 or more individuals be reported to HHS as well, in certain circumstances, as major media in the area.[32]

However, as healthcare systems have moved more and more into the electronic realm, the bigger target for hackers they have become: while 2014 saw 68% of healthcare data breaches result from theft or loss of employee devices, in 2015 98% of all breaches of data came from hacking.[33] It has been estimated that over the past three years, 40% of all data breaches in the United States came from the healthcare industry.[34] Additionally, 91% of all health organizations have reported a data breach within the last two years.[35]

The federal government has repeatedly attempted to halt the rise of cyberattacks on the US healthcare system. In 2013, President Obama issued Executive Order 13636, calling for the development of increased cybersecurity for critical cyber-infrastructure, including the healthcare industry.[36] In 2016, the President also issued a factsheet related directly to the issue of cybersecurity that laid out a detailed plan for how to deal with the issue that would include over a three billion dollar information technology modernization stimulus, the creation of more cyber defense teams for DHS, and further investment in cybersecurity education.[37] Even a Congressional bill on cybersecurity included a section dedicated purely to improving cybersecurity standards in the healthcare industry.[38]

Despite increased awareness and guidelines on the issue, cybersecurity continues to be something the healthcare industry as a whole grapples with. In 2015 alone, 113 million electronic health records were compromised, and in 2016, the industry has averaged 4 reportable data breaches per week.[39]

[https://perma.cc/9E2S-BE6G] (last updated Dec. 2014).

32. *HIPAA/HITECH Enforcement Action Alert*, THE NAT'L L. REV. (Mar. 22, 2012), http://www.natlawreview.com/article/hipaahitech-enforcement-action-alert [https://perma.cc/V9H7-9T96].

33. Heather Landi, *Hacking Accounted for 98 Percent of Healthcare Data Breaches in 2015, Report Says*, HEALTHCARE INFORMATICS (Feb. 1, 2016), http://www.healthcare-informatics.com/news-item/hacking-accounted-98-percent-healthcare-data-breaches-2015-report-says [https://perma.cc/T7FS-RGPB].

34. *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework*, U.S. DEP'T. OF HEALTH & HUMAN SERVS. (Feb. 23, 2016), (http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/ [https://perma.cc/MZV3-RAXM].

35. *Id.*

36. Improving Critical Cybersecurity Infrastructure, 78 Fed. Reg. 11737 (Feb. 12, 2013).

37. OFFICE OF THE PRESS SECRETARY, FACT SHEET: CYBERSECURITY NATIONAL ACTION PLAN (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [https://perma.cc/U5KX-9E5X].

38. S.754, 114th Congr. § 405 (2015).

39. Nsikan Akpan, *Has health care hacking become an epidemic?*, PBS (Mar. 23, 2016, 6:19 PM), http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/

D. Rise of Ransomware as a Critical Threat

Ransomware has been around since the 1980's, but the rise of cyber-currency such as Bitcoin has given hackers an anonymous way to receive payment without fear of discovery, and thus has fueled ransomware's resurgence.[40] This is not news to most information technology security firms, who have been warning healthcare organizations of the threat ransomware poses to their information for years now that:

> "Ransomware has been an inconvenient truth for a while, a tried and tested dance where an attack is launched and the ransom is modest, just enough where many organizations pay it to make the problem go away…[b]ut demands for funds are soaring, and the problem is organizations are paying. Ransomware will get worse before it gets better."[41]

Incidents involving ransomware have only grown more prevalent as time has gone on.[42] As of 2016, there have been over 4,000 daily ransomware attacks, a 300% increase from 2015.[43] It is estimated that by the end of 2016, hackers will have pulled in an estimated one billion dollars using ransomware, making it an incredibly lucrative business.[44]

Hospitals are now one of the most heavily targeted places, with nearly half of all U.S. hospitals reporting at least one ransomware attack in the past year.[45] Although the FBI has publicly advised hospital systems against paying the ransom,[46] it has also admitted that paying the ransom may be a necessity in order to regain access to patient records.[47] As one FBI representative cynically summed

---

[https://perma.cc/69TB-D5YD].

40. Sneed, *supra* note 19.

41. Bill Siwicki, *Tips for protecting hospitals from ransomware as cyberattacks surge*, HEALTHCARE IT NEWS (Apr. 6, 2016, 6:59 AM), http://www.healthcareitnews.com/news/tips-protecting-hospitals-ransomware-cyber-attacks-surge [https://perma.cc/V768-RQAD].

42. *See also* Stu Skouwerman, *Ransomware on the rise: The evolution of a cyberattack*, TECH BEACON (Nov. 5, 2016), http://techbeacon.com/ransomware-rise-evolution-cyberattack [https://perma.cc/TU9B-4632] (establishing the timeline of ransomware attacks).

43. U.S. DEP'T. OF HEALTH & HUMAN SERVS, *supra* note 4.

44. Danny Palmer, *The cost of ransomware attacks: $1 billion this year*, ZD NET (Sept. 8, 2016, 11:46 GMT), http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/ [https://perma.cc/E8CN-BBKM].

45. Steven D. Gravely & Erin S. Whaley, *Ransomware in Healthcare – A Clear and Present Danger*, TROUTMAN SANDERS (July 14, 2016), https://www.troutmansanders.com/ransomware-in-healthcare---a-clear-and-present-danger-07-14-2016/ [https://perma.cc/8F3J-CP6Z].

46. *Incidents of Ransomware on the Rise*, FED. BUREAU OF INVESTIGATION (Apr. 29, 2016), https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise [https://perma.cc/6UNH-AULY].

47. *FBI's Advice on Ransomware? Just Pay the Ransom.*, THE SECURITY LEDGER (Oct. 22,

up, "To be honest, we often advise people just to pay the ransom."[48] It has been estimated that for every unplanned downed minute away from data centers, a hospital can lose an average of $7,900 per minute, further incentivizing prompt payment.[49] This accounts for both direct and indirect costs of downtime away from data, and includes factors such as equipment damage, loss in confidence among consumers, as well as other costs including legal fees and HIPAA penalties for a breach.[50] Even if the hospital goes without paying the ransom, it can still lead to several days' worth of delays while hospitals attempt to clean out their network, which can compromise patient safety and lead to inefficient treatment.[51] It is perhaps no wonder, then, that there is a temptation to pay the ransom in short order: the average incident involving downtime spent as a result of inaccessible data—only 86 minutes—can cost a hospital a total of $690,200.[52]

So far in 2016, there have been three major, publicized attacks on hospitals that paint a disturbing picture of increased boldness and sophistication by the attackers. The attack on Medstar in March, regarded as the most damaging attack of the year, effectively forced 10 hospitals and 250 outpatient centers to shut down their computer network, delay treatments and appointments, and turn away thousands of patients to other hospitals.[53]

The grim situation that the medical staff faced without the ability to access the medical information of their patients was well encapsulated by the media: "Without access to email and computer systems, the medical staff fell back on seldom-used paper records that had to be faxed or hand-delivered. But…[t]hey can be missing vital pieces of patient information: complete medical histories, every drug prescribed, allergies to medicine and treatment plans."[54] Medstar personnel were quick to assure that no patient records were illegally accessed by third parties during the crisis.[55] Evidence later indicated that while the IT

2015), https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom [https://perma.cc/DN6N-YXXE].

48. *Id.*; *see also* Haley Sweetland Edwards, *A Devastating Type of Hack Is Costing People Big Money*, TIME (Apr. 21, 2016), http://time.com/4303129/hackers-computer-ransom-ransomware/ [https://perma.cc/X9EW-56R9].

49. Kacy Zurkus, *The rise of ransomware in healthcare*, CSO (July 11, 2016, 3:50 AM), http://www.csoonline.com/article/3091080/security/the-rise-of-ransomware-in-healthcare.html#*slide4* [https://perma.cc/6VCD-QW55].

50. *See generally* Yevgeniy Sverdlik, *One Minute of Data Center Downtime Costs US$7,900 On Average*, DATACENTER DYNAMICS (Dec. 4, 2013), http://www.datacenterdynamics.com/content-tracks/power-cooling/one-minute-of-data-center-downtime-costs-us7900-on-average/83956.fullarticle [https://perma.cc/6VCD-QW55].

51. Brian Contos, *Ransomware attacks force hospitals to stich up networks*, CSO (May 19, 2016, 8:24 AM), http://www.csoonline.com/article/3072503/backup-recovery/ransomware-attacks-force-hospitals-to-stitch-up-networks.html [https://perma.cc/7GDY-X4BQ].

52. *See generally* Sverdlik, *supra* note 50.

53. Cox, *supra* note 1.

54. *Id.*

55. *Id.*

department was not at fault, an improperly installed server likely created a vulnerability in their cybersecurity suite and gave hackers an ability to bypass cybersecurity measures in place.[56]

In another notable incident, Hollywood Presbyterian Medical Center in Los Angeles was forced to pay approximately seventeen thousand dollars-worth of bitcoins after ransomware locked medical personnel out of its patient records.[57] The hospital paid the ransom, viewing it as "the quickest and most efficient way to restore…operations.", but even after a week of being locked out of their electronic health records while hospital staff attempted to remove the ransomware from their systems,[58]neglected to inform local or federal law enforcement of the attack until after they had already paid.[59] Hospital management claims that hospital records were never accessed during the attack, but medical personnel were forced to revert back to pen and paper to continue hospital functions.[60]

A similar event happened in Kansas later in 2016. Kansas Heart Hospital, despite being aware of the looming threat ransomware was posing upon the industry and taking the time to have a plan in place in case they were ever attacked, was hit with ransomware and was still forced to pay a ransom in order to ensure the release of its patient data.[61] Afterward, rather than unlocking the data, the hackers demanded a second ransom payment of an undisclosed amount.[62] The hospital balked at this second demand after outside consultants advised against paying any additional ransom fee.[63] While its data was returned shortly thereafter, the attack on Kansas Heart Hospital may portend future additional extortions from attackers against hospitals, even when they pay the ransom.[64]

Until the HHS announcement in summer 2016 specifically regarding ransomware,[65] there were concerns that because in many of these situations no technical breach of electronic PHI occurs, hospitals would simply pay the ransom

---

56. Sean Gallagher, *Maryland hospital: Ransomware success wasn't IT department's fault*, ARS TECHNICA (Apr. 7, 2016, 10:12 AM), https://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomware-attack/ [https://perma.cc/2DSR-MYFD].

57. Richard Winton, *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*, L.A. TIMES (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html [http://perma.cc/H5D7-PF2N].

58. Green, *supra* note 6.

59. Winton, *supra* note 57.

60. *Id.*

61. 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 [http://perma.cc/9Y63-KZ6W].

62. *Id.*

63. *Id.*

64. *Id.*

65. *See generally* U.S. DEP'T. OF HEALTH & HUMAN SERVS, *supra* note 4.

and not report any breach of patient data.[66]

E. The U.S. Federal Government's Response to the Growing Threat of HIPAA Data Breaches

After months of major ransomware attacks across the country, Congress pushed to get HHS to recognize ransomware attacks as breaches.[67] Representatives Ted Lieu (D, Cal.) and Will Hurd (R, Tex.) sent a letter to the OCR requesting that it recognize ransomware attacks as some sort of breach.[68] In this letter, both congressmen acknowledged the unusual nature of the threat ransomware poses, wherein ransomware is largely a problem towards patient safety rather than privacy, but requested clarification and guidance from the HHS.[69]

Finally, in the summer of 2016, HHS released a fact sheet for the healthcare industry that outlined how it views ransomware attacks.[70] Its response provided basic answers regarding ransomware, including how it defines ransomware, how HIPAA compliance could help protect covered entities, and what to do if an organization found itself on the receiving end of an attack.[71]

In addition to that information, HHS also provided some crucial insight as to what it considers a ransomware attack to be in regards to HIPAA.[72] Effectively, HHS considers any successful ransomware attack to be a breach of PHI, and therefore requires the covered entity to make a report to HHS under HIPAA.[73] In several sections throughout the fact sheet, HHS explicitly states that HIPAA compliance ¾with measures such as creating and maintaining quality backup copies of data off of the network, emergency disaster recovery and operations planning, and reviewing cybersecurity measures already in place¾is enough to

---

66. Dan Munro, *Is Ransomware Considered A Health Data Breach Under HIPAA?*, FORBES (Mar. 29, 2016, 9:26 PM), http://www.forbes.com/sites/danmunro/2016/03/29/is-ransomware-considered-a-health-data-breach-under-hipaa/#12b8d5cd597d [http://perma.cc/8HBB-8N44].

67. Elizabeth Snell, *Reps Push for Stronger Healthcare Ransomware Guidance*, HEALTH IT SECURITY (July 7, 2016), http://healthitsecurity.com/news/reps-push-for-stronger-healthcare-ransomware-guidance [http://perma.cc/MU7A-H7WU]; *see also* Elizabeth Snell, *Senator Urges HHS to Create Healthcare Cybersecurity Law*, HEALTH IT SECURITY (Mar. 30, 2016), http://healthitsecurity.com/news/senator-urges-hhs-to-create-healthcare-cybersecurity-law [http://perma.cc/W5HC-8E48].

68. U.S. Representative Ted Lieu, *Representatives Lieu and Hurd Urge HHS to Hone Focus On Ransomware Guidance*, PRESS RELEASE (June 28, 2016),
https://lieu.house.gov/media-center/press-releases/representatives-lieu-and-hurd-urge-hhs-hone-focus-ransomware-guidance [http://perma.cc/3T4A-LX52].

69. *Id.*

70. *See generally* U.S. DEP'T. OF HEALTH & HUMAN SERVS., *supra* note 4.

71. *See generally id.*

72. *See generally id.*

73. *Id.*at 5, 6.

prevent or mitigate a ransomware attack.[74] HHS also clarified its stance on how an organization can show that a breach had not occurred even if an attack is successful, but made it clear that its default position would require a fact-specific analysis to prove that no breach has occurred.[75] In other words, an attack is to be reported as if it were a breach unless a covered entity can demonstrate a low probability of a breach.[76]

HHS took several steps to justify this conclusion. HHS considers ransomware to constitute a security incident under HIPAA; "[a] security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[77] The HIPAA Breach Notification Rule defines "breach" as "'the acquisition, access, use, or disclosure of PHI in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.'"[78] Because a hacker who has used ransomware has technically "acquired" the information, HHS views this as a reportable breach.[79] However, the savings clause of this same section also provides that if the covered entity believes the chances of a breach of PHI to be low, defined as not something that was defined or given an objective standard other than the four-part test within the HHS ransomware memo,[80] they may conduct the following risk assessment test using the guidelines mentioned earlier in this Note:

> (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
> (2) the unauthorized person who used the PHI or to whom the disclosure was made;
> (4) whether the PHI was actually acquired or viewed; and
> (5) the extent to which the risk to the PHI has been mitigated.[81]

In addition to the rules laid out in the Savings Clause, HHS has also outlined three general exceptions to the breach notification rule:

> The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.[82] The second exception applies to the inadvertent disclosure

---

74. *Id.*at 2, 3.
75. *Id.* at 6.
76. *Id.* at 6.
77. *Id.* at 4.
78. *Id.* at 5.
79. *Id.* at 5-6.
80. *Id.* at 6.
81. *Id.*
82. *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS.,

> of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.[83] The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information."[84]

A reportable breach also opens up a covered entity to mandatory financial penalties under HIPAA, which can range anywhere from $100 to $1,500,000 depending on the severity of the breach and the whether the covered entity had "willful[ly] neglect[ed]" to comply with HIPAA.[85] These penalties can be waived, but it is entirely at the discretion of the OCR, and is otherwise a normal consequence of a breach.[86]

These exceptions to the Breach Notification Rule create a highly fact-specific examination where hospitals and other covered entities must determine whether or not to notify HHS of a breach based off of whether they believe the patient data in their hands was legitimately compromised or not. Whether or not the data has actually been transferred to the responsible party or not depends entirely on the variant of ransomware utilized.[87] Most variants, as of now, do not actually exfiltrate their data to a third-party.[88] Instead, they merely lock out users until a ransom has been paid.[89] On top of that, determining which variant of ransomware a covered entity has been hit by can be difficult without the right technical support, something the healthcare industry does not currently have at its disposal.[90] This is not a workable framework going forward, and must be changed

---

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/NG97-LSLP].

83. *Id.*

84. *Id.*

85. *What Are the Penalties for HIPAA Violations?* HIPAA J. (June 24, 2015), http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ [https://perma.cc/F9NH-FNHL].

86. *Id.*

87. *See generally* Mellen, *supra* note 7 (explaining how HHS requires an analysis of ransomware to determine if data exfiltration has occurred, a capability that is not currently widely available); *but see* Andra Zaharia, *What is Ransomware and 15 Easy Steps to Keep Your System Protected*, HEIMDAL SECURITY (July 7, 2016), https://heimdalsecurity.com/blog/what-is-ransomware-protection/ (describing the many capabilities ransomware can possess, including exfiltration). [https://perma.cc/7UCZ-ESEJ].

88. Mellen, *supra* note 7.

89. *Id.*

90. *Id.*

to allow for more clarification on when a healthcare provider is required to report instead of allowing for a greater amount of leeway.

B. The Response of Other Countries to the Growing Threat of Healthcare-Related Data Breaches

1. The European Union

Countries within the European Union have also suffered ransomware attacks in recent years, although nothing as high profile as any of the recent attacks in the United States.[91] However, European Union nations have also proved more reluctant to pay hackers when they have been directly threatened. Despite successful ransomware infections in hospitals throughout the United Kingdom, adequate preexisting safety measures allowed hospitals within the United Kingdom's National Health Service to avoid paying a ransom and to resume normal operations in relatively short order.[92] Similarly, hospitals in Germany have also suffered ransomware attacks, but were able to avoid paying by shutting down their systems and relying on backup data.[93] Cooperation between private entities and public law enforcement has also helped educate entities within the European Union as to how best to combat ransomware.[94]

Unlike the United States, the European Union has explicitly enshrined the protection of personal data, including personal health information, in both its Treaty on the Functioning of the European Union as well as its Charter of Fundamental Human Rights.[95] This has generally led to increases in privacy protection as a result, leaving the European Union better prepared to meet threats to patient data protection in the healthcare industry:[96]

> The EU framework begins with the presumption of privacy for sensitive health records. In a sense an electronic health system of collection and sharing must then prove itself to meet those privacy standards. . . . [I]n

---

91. John Leyden, *Medical superbugs: Two Germany hospitals hit with ransomware*, THE REGISTER (Feb. 26, 2016, 5:08 PM), http://www.theregister.co.uk/2016/02/26/german_hospitals_ransomware/. [https://perma.cc/2UQE-YL5U].

92. Joseph Cox, *Ransomware Targets UK Hospitals, But NHS Won't Pay Up*, MOTHERBOARD (Aug. 30, 2016, 8:30 AM), http://motherboard.vice.com/read/ransomware-targets-uk-hospitals-but-nhs-wont-pay-up [https://perma.cc/HR99-PMCM].

93. Leyden, *supra* note 91.

94. *No More Ransom: Law Enforcement And IT Security Companies Join Forces to Fight Ransomware*, EUROPOL (July 25, 2016), https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware. [https://perma.cc/4S3G-5CP4].

95. EUROPEAN COMMISSION, DATA PROTECTION IN THE EU, http://ec.europa.eu/health/data_collection/data_protection/in_eu/index_en.htm. [https://perma.cc/L9JH-PALF].

96. Janine Hiller, et. al, *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared*, 17 B.U.J. SCI. & TECH. L.1 (2011).

> comparison, the U.S. framework, while making progress in the protection of health information, lacks the historical presumption of privacy[.][97]

Until recently, the European Union's primary data protection law was based around Directive 95/46/EC.[98] This directive allowed the individual member-states to create their own data protection legislation, so long as they adhered to the minimum standards laid out by the directive, including adhering to its definition of personal data and the principles by which data was to be protected.[99] In an effort to harmonize data protection across the Union, European Union lawmakers recently passed the General Data Protection Regulation, designed to simultaneously simplify the regulatory environment and provide greater security to personal data.[100] It is due to become the law of the land in 2018.[101] The sanctions specified in the new regulation are not automatically enforced upon a breach, but can be incredibly punishing for the worst offenders: in the worst cases, an offending corporation may be liable for up to 4% of their total worldwide profit.[102] Additionally, while the new regulation requires more prompt reporting to the supervisory authorities and affected persons, it does not mandate a public reporting requirement to local media as HIPAA does for data breaches in the United States;[103] as a result, this may make it more difficult to determine the prevalence of ransomware in European Union nations.[104]

2. Australia & New Zealand

Australia and New Zealand have also seen a significant spike in ransomware attacks against their healthcare infrastructure as healthcare information has become more digital. Despite its more modestly-sized economy and population compared to economic powerhouses such as the United States or European Union, Australia still suffered 6% of all global ransomware detections in the first quarter of 2015, the second highest number in the world.[105] Most notably in the

---

97. *Id.*

98. Council Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), (EC) [hereinafter Data Protection Directive].

99. *Id.*

100. Regulation 2016/679 on the Protection of Natural Persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter General Data Protection Regulation].

101. *Id.* at 87.

102. *See* General Data Protection Regulation, 2016 O.J. L.119, 2016/679.

103. *Id.*

104. *See generally* Laurens Cerulus, *Hackers hold the health care sector ransom*, POLITICO (Nov. 29, 2016, 5:01 PM CET), http://www.politico.eu/article/ransomware-in-health-care-draft/ (explaining that stricter data breach notification requirements make ransomware a more visible problem in the US than in the European Union) [https://perma.cc/7E29-9E5D].

105. Bonnie Gardiner, *Australia records 6 per cent of global ransomware detections*, CIO (May 21, 2015), http://www.cio.com.au/article/575500/australia-sees-second-highest-number-ransomware-attacks-q1-2015/ [https://perma.cc/KH8A-W6ZR].

healthcare field, the Royal Melbourne Hospital was targeted by cybercriminals in 2016;[106] while the strain of malware utilized in the attack did not actually carry ransomware, cyber security experts have warned that this strain is now capable of delivering a ransomware attack if a hacker modifies the malware accordingly.[107] Despite having a population six times smaller than Australia, New Zealand also suffered a high-profile ransomware attack in 2016, when the Whanganui District Health Board was targeted by Russian cybercriminals.[108] Despite a brief outage, the Health Board was able to contain the ransomware virus and paid no ransom to the hackers.[109]

Although both nations have suffered attacks, they also have very strong data protection laws governing the healthcare field. In particular, Australia's Privacy Act of 1988, their HIPAA equivalent, has very stringent terms regarding the security of health information, including a broad definition of health services that includes any entity holding onto health information for the purposes of assessing, maintaining, improving, or managing a person's health.[110] There are, however, some structural reasons why Australia and New Zealand see a seemingly disproportionate number of attacks in spite of their smaller economies. First, organizations in both countries are the most likely to employ data protection strategies that merely monitor, rather than monitor and block, ransomware incidents, meaning that while initial detection is strong, countermeasures for an actual attack likely come down to the preparation of the individual organization rather than compliance with data protection laws.[111] Organizations within the United States, in contrast, are the most likely to employ a monitor and block

---

106. Zak Khan, *Healthcare held to ransom: how to protect Australian healthcare systems and patients from cybercrime*, CSO (April 1, 2016), http://www.cso.com.au/article/597125/healthcare-held-ransom-how-protect-australian-healthcare-systems-patients-from-cybercrime/ [https://perma.cc/2A6F-BPKD].

107. *See* Tom Spring, *Qbot Malware Morphs Quickly to Evade Detection*, THREAT POST (Apr. 13, 2016, 1:28 PM), https://threatpost.com/qbot-malware-morphs-quickly-to-evade-detection/117377/ [https://perma.cc/6MQJ-FYTG].

108. Sophie Ryan, *Hackers attack hospital system*, WANGANUI CHRON. (Feb. 24, 2016, 8:39 AM), http://www.nzherald.co.nz/wanganui-chronicle/news/article.cfm?c_id=1503426&objectid=11594628 [https://perma.cc/5PG5-JHGC].

109. *Id.*

110. *Health Information and Medical Research*, OFFICE OF THE AUSTRALIAN INFO. COMMISSIONER (last viewed Mar. 15, 2017), https://www.oaic.gov.au/privacy-law/privacy-act/health-and-medical-research [https://perma.cc/NK52-ZX8L].

111. Shannon Williams, *Ransomware and mobile malware hits peak, healthcare least prepared,* SECURITY BRIEF NZ (Sep. 21, 2016), https://securitybrief.co.nz/story/ransomware-and-mobile-malware-hits-peak-healthcare-least-prepared/ [https://perma.cc/UV5Y-DH2U]; *see also* Grame Burton, *Australian government might force ISPs to block malware and websites associated with online scams*, V3 (Apr. 26, 2017), https://www.v3.co.uk/v3-uk/news/3009069/australian-government-might-force-isps-to-block-malware-and-websites-associated-with-online-scams [https://perma.cc/X86T-G66A].

strategy.[112] Additionally, despite how stringent their health information laws are, neither Australia nor New Zealand currently have any data breach reporting requirements on the books, [113] although both countries are mulling provisions that would make reporting mandatory under certain conditions.[114] If passed, these laws could help shed more light on the number of ransomware attacks actually occurring against Australia and New Zealand, and lead to further measures being taken to bolster cybersecurity laws already in place.

3. Canada

Canada has not been immune to the scourge of ransomware either, suffering over 1,600 ransomware attacks per day in 2015.[115] The Canadian healthcare system has also been targeted by ransomware attackers, with one high profile attack occurring in Ottawa in spring of 2016.[116] Each ransomware incident costs Canadian hospitals approximately $355,[117] and it is estimated that health IT in the nation is approximately five years behind the IT capabilities of other industries.[118] On top of that, Canadian companies and entities are also more willing to pay the ransom when asked, being 75% more likely to pay the ransom demand than other countries.[119] In spite of that, Canadians feel more confident in their data protection systems than their American counterparts, with 51% of Canadians feeling confident in their ability to stop ransomware despite 72% of Canadian companies suffering a ransomware attack in 2015.[120]

Canadian healthcare entities are similar in preparation level to their United

---

112. *Id.*

113. Mandy Simpson, *Healthcare providers face rising cyber security risks in 2017*, CYBER TOA (Jan 16, 2017), https://medium.com/cyber-toa/healthcare-providers-face-rising-cyber-security-risks-in-2017-b8d6ad6c895b [https://perma.cc/294D-FYTN].

114. Jeremy Kirk, *Australia, New Zealand Still Milling Data Breach Laws*, BANK INFO SECURITY (May 24, 2016), http://www.bankinfosecurity.com/australia-new-zealand-still-mulling-data-breach-laws-a-9134 [https://perma.cc/4Q5E-E35T].

115. Nicole Bogart, *Ransomware on the rise in Canada: How to protect your data*, GLOBAL NEWS (April 17, 2016, 9:00 AM) http://globalnews.ca/news/2641249/ransomware-on-the-rise-in-canada-how-to-protect-your-data/ [https://perma.cc/ANZ2-9Z9Q].

116. *Ottawa Hospital hit with ransomware, information on four computers locked down*, NAT'L POST (March 13, 2016, 2:10 PM EDT), http://news.nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down [https://perma.cc/T2TB-DUSR].

117. David Masson, *Protecting Patient Information in Modern Health Care*, HUFFINGTON POST CAN. (Jan. 27, 2017, 4:59 AM EST), http://www.huffingtonpost.ca/david-masson/protecting-patient-information_b_14419396.html [https://perma.cc/GGV9-7XG7].

118. Christine Wong, *The unhealthy state of CIO influence in Canadian health care*, IT WORLD CANADA (June 30, 2015), http://www.itworldcanada.com/article/the-unhealthy-state-of-cio-influence-in-canadian-health-care/375654 [https://perma.cc/3SCU-YBUP].

119. Nathan Kornet, *Are Canadian Companies Really Prepared for Ransomware?* ASIGRA: BLOG (Feb. 8, 2017) http://www.asigra.com/blog/are-canadian-companies-really-prepared-ransomware# [https://perma.cc/N8AM-24BB].

120. *Id*.

States counterparts; 96% of American companies were not very confident in their ability to stop a ransomware attack, and only 9% of Canadian organizations out of 103 surveyed were deemed to be highly secure and prepared for any sort of cyberattack.[121] Canadian laws regulating the private sector in regards to data protection are similar to those found in the European Union.[122] Unlike either the United States or the European Union however, Canada has only recently passed a bill that would require entities to notify individuals of a breach of their personal health information.[123] This new law would also require private entities to keep track of data breaches, even if they would not ordinarily constitute a reportable breach.[124]

II. ANALYSIS: THE DECISION BY HHS DOES NOT ADEQUATELY MEET THE CHALLENGES IMPOSED BY RANSOMWARE

A. Reaction to the HHS Announcement

1. Federal Government

Congress has contemplated passing legislation that would force HHS to recognize ransomware attacks as reportable data breaches,[125] as well as legislation that would further criminalize the usage of ransomware and other similar malware attacks.[126] Thus far, such legislation has stalled. In terms of overall cybersecurity, Congress has only passed one major cybersecurity investment package, which took five years to assemble and neglected to include ransomware as a chief threat.[127] Digital education, or lack thereof, seems to play a key part in why

---

121. Oliva Bowden, *Canadian companies are vulnerable to the increasing risk of cyber attacks*, FINANCIAL POST (Aug. 29, 2016, 5:00 AM EST), http://business.financialpost.com/executive/smart-shift/canadian-companies-are-vulnerable-to-the-increasing-risk-of-cyber-attacks [https://perma.cc/9Q9Y-W2HQ]; *see also International Study Finds Nearly 40 Percent of Enterprises Hit By Ransomware in the Last Year*, MALWAREBYTES (Aug. 3, 2016), https://press.malwarebytes.com/2016/08/03/international-study-finds-nearly-40-percent-of-enterprises-hit-by-ransomware-in-the-last-year/ [https://perma.cc/XPU6-HXPN] (stating that 96% of American organizations are not confident in their ability to prevent ransomware attacks).

122. Timothy M. Banks & Karl Schober, *Data Security and Cybercrime in Canada,* LEXOLOGY (Sept. 25, 2016), http://www.lexology.com/library/detail.aspx?g=237135ad-df34-4e79-87fa-554b3dfdc7fa [https://perma.cc/7EG4-VMAZ].

123. *Id.*

124. *Id.*

125. Dennis Fisher, *Ransomware Attacks Mat Trigger Breach Notifications*, ON THE WIRE (June 28, 2016), https://www.onthewire.io/ransomware-attacks-may-trigger-breach-notifications/ [https://perma.cc/DHZ2-FKRN].

126. Sean Lyngaas, *With ransomware on the rise, Senate botnet bill gets another shot*, FCW (May 19, 2016), https://fcw.com/articles/2016/05/19/botnet-whitehouse-bill.aspx [https://perma.cc/7ZSK-CBLC].

127. Cory Bennett, *Congress approves first major cyber bill in years*, THE HILL (Dec. 18, 2015, 12:07 PM EST), http://thehill.com/policy/cybersecurity/263696-congress-approves-first-

government has been hesitant to tackle this issue more heavily.[128] The Pell Center for International Relations and Public Policy, which authored a report on cybersecurity issues, came to the conclusion that a lack of cyber-education within Congress was largely responsible for why more has not been done to provide cybersecurity assistance, stating:

> Most legislators are poorly educated on these issues and very few have taken the time to understand how this helps a state economically or from a security standpoint . . . [w]e see the same issues in state legislatures that we see in the U.S. Congress. Although it is a bipartisan issue, the reason so many cybersecurity bills are stalling in Congress comes down to those who have taken the time to educate themselves and those who haven't.[129]

This lack of education has effectively meant that Congress only acts when a major cyberattack is in the public spotlight, something that led the executive director of the National Association of State Chief Information Officers to remark that, "[I]t often takes a data breach for lawmakers to pass significant legislation around cybersecurity. . . ."[130] The high-profile nature and large volume of ransomware attacks, as well as other major cybersecurity breaches, in both the United States and abroad has helped provide more long-standing attention to the situation.

This is something that industry analysts hope will prompt Congress to take more action:

> You always want to take advantage of somebody else's breach to educate. It does bring home the fact that you either invest in front of the problem or you are investing by trying to clean up at the back end of the problem. It is a tough job to find out where that balance is. It is important to me that we don't spend our tax dollars cleaning up something that could have been avoided.[131]

In 2015, Congress established a temporary Cybersecurity Task Force to consult on cybersecurity threats facing the healthcare industry, which it began working on in 2016.[132] The Task Force reported on its findings to Congress in June of

---

major-cyber-bill-in-years [https://perma.cc/G45U-2J5D]; *see also* Sean Lyngaas, *With ransomware on the rise, Senate botnet bill gets another shot*, FCW (May 19, 2016), https://fcw.com/articles/2016/05/19/botnet-whitehouse-bill.aspx [https://perma.cc/7ZSK-CBLC].

128. David Raths, *Legislating Cybersecurity: Breaches Grab Lawmakers' Attention*, GOVERNMENT TECH. (Oct. 12, 2016), http://www.govtech.com/security/Legislating-Cybersecurity-Breaches-Grab-Lawmakers-Attention.html [https://perma.cc/M6D5-RZFY].

129. *Id.*

130. *Id.*

131. *Id.*

132. *Health Care Industry Cybersecurity Task Force*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (last viewed Feb. 10, 2017), https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx [https://perma.cc/CXC8-SVSU].

2017.[133]

2. The Healthcare Industry

Thus far, most of the healthcare industry, particularly in the legal field, has largely focused on helping that covered entities comply with the HIPAA-based ransomware guidance recommended by HHS.[134] Part of this awareness and stress for HIPAA compliance comes from the potential punishments: covered entities are now effectively on notice that failure to take reasonable precautions to prevent ransomware will lead to HIPAA penalties.[135] Outside of these actions, there are no perceptible changes being done within most covered entities to upgrade their cybersecurity systems, and continued ransomware attacks seem to indicate that this will be a growing problem until fundamental changes are made.

B. Problems with the HHS Response

The HHS guidelines certainly illuminate its thoughts on why it has categorized ransomware as causing breaches, and gives covered entities some guidance on how to proceed in the immediate future; however, even with the HHS guidelines and recommendations designed to help hospitals shore up their security systems, current ransomware trends indicate that complying with HIPAA will not be enough to thwart future ransomware attacks in the coming years.

For one, ransomware software is becoming more and more sophisticated to get around the HHS recommendations regarding "phishing" tactics, or attacks that ask for your personal information.[136] For example, a variant of ransomware known as "Locky" disguises itself as an email claiming to carry a legitimate office invoice.[137] Newer variants of ransomware are now being found that target network backups, further negating current strategies to keep an online backup.[138] Some variants no longer even require an individual to open up a malicious email; ransomware can now be seeded into legitimate websites and take advantage of unpatched software.[139] Even if a covered entity's personnel are trained against clicking on suspicious links, there is always the threat that a hacker can access a

---

133. HEALTH CARE INDUS. CYBERECURITY TASK FORCE, REP. ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUS. (2017).

134. *See generally HHS Issues New Guidance on Ransomware*, ROPES & GREY (July 19, 2016), https://www.ropesgray.com/newsroom/alerts/2016/July/HHS-Issues-New-Guidance-on-Ransomware.aspx [https://perma.cc/6XAB-QTJE] (providing an example of a law firm explaining how covered entities need to treat HHS ransomware guidance).

135. Elizabeth Snell, *HIPAA Data Breaches: What Covered Entities Must Know*, HEALTH IT SECURITY, http://healthitsecurity.com/features/hipaa-data-breaches-what-covered-entities-must-know [https://perma.cc/M5MD-RVV5] (last visited Nov. 5, 2016).

136. FED. TRADE COMMISSION, CONSUMER INFORMATION: PHISHING, https://www.consumer.ftc.gov/articles/0003-phishing [https://perma.cc/MFB3-DM2N] (last updated July 2017).

137. Zetter, *supra* note 21.

138. *Id.*

139. FED. BUREAU OF INVESTIGATION, *supra* note 46.

covered entity's network through a jump-drive.[140] In a recent DHS test, staffers discreetly dropped computer disks and jump drives in various government buildings and parking lots; 60% of those items ended up being plugged into government computers, and the percentage rose to almost 90% when those items had an official logo.[141] Even the best network defenses can fall prey to human error.

Secondly, covered entities, specifically hospitals, are already notoriously behind the times in terms of their technology and cybersecurity. Hospitals are largely still wired with unprotected wireless access and outdated computer operating systems, which facilitate easy attacks by hackers.[142] The plethora of medical devices within a hospital that are largely unprotected also grant an access point to external attackers.[143] In essence, a covered entity simply has too many holes in its cybersecurity defenses to effectively cover all of them.

Even if a covered entity goes above and beyond in complying with HIPAA and fully and appropriately encrypts its data, this is no guarantee that a covered entity can presume that there was no breach. The Health and Human Services guidelines themselves serve to indicate that point, stating:

> Because [decryption occurred] and thus [became] "unsecured PHI" at the point in time that the ransomware accessed the file, an impermissible disclosure of PHI was made and a breach is presumed. Under the HIPAA Breach Notification Rule, notification in accordance with 45 CFR 164.404 is required unless the entity can demonstrate a low probability of compromise of the PHI based on the four-factor risk assessment.[144]

This proclamation from HHS serves to indicate that even if a covered entity has taken every foreseeable means to protect its data from a ransomware attack, if an attack does occur and successfully overwrites the cybersecurity encryptions of a covered entity's PHI, then a breach has still occurred and will be presumed unless the covered entity in question can prove otherwise. As ransomware overwrites any data encryption with its own encryption,[145] this scenario effectively applies to every situation involving ransomware and thus will always mean that a covered entity must conduct a risk assessment. While this policy is very patient-friendly and leans on the side of protecting the health information of the public, it simultaneously creates an unattainable standard for covered entities,

---

140. Siwicki, *supra* note 41.

141. *Id*; *see also* Lisa Vaas, *Hospitals vulnerable to cyber attacks on just about everything*, NAKED SECURITY BY SOPHOS (Feb. 26, 2016), https://nakedsecurity.sophos.com/2016/02/26/hospitals-vulnerable-to-cyber-attacks-on-just-about-everything/ [https://perma.cc/XHE6-F644] (describing a similar test involving healthcare facilities).

142. *Cybersecurity in the Healthcare Industry*, INFOSEC INSTITUTE (May 23, 2016), http://resources.infosecinstitute.com/cybersecurity-in-the-healthcare-industry/ [https://perma.cc/B67V-J5Z9].

143. *Id.*

144. U.S. DEP'T. OF HEALTH & HUMAN SERVS., *supra* note 4.

145. *Id.*

who will always be open to financial penalties under HIPAA should a breach occur in spite of any efforts taken to go beyond what HIPAA currently stipulates. In effect, it indirectly creates a disincentive to strengthen cybersecurity.

In addition to the technical difficulties encountered by covered entities, the current HHS position that ransomware is a breach creates too many loopholes for covered entities to avoid reporting breaches, potentially leading to underreporting of an issue that affects every American. The aforementioned four factors that HHS determined must be met in order for a covered entity to determine that no breach had occurred are essential in this task. Those four factors are:

(1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(2) the unauthorized person who used the PHI or to whom the disclosure was made;
(3) whether the PHI was actually acquired or viewed; and
(4) the extent to which the risk to the PHI has been mitigated.[146]

However, HHS has also declared that there are other exceptions to the breach rule, most importantly the "good faith belief" exception. "The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information."[147] Determining which of the hundreds of variants of ransomware a covered entity was hit by–and consequently whether or not the lost data was actually viewed by a third party–might not be realistic to do. This in turn might incentivize covered entities to claim that there was no breach based on good-faith belief, which would enable them to avoid opening themselves up to HIPAA fines and penalties for failure to prevent a breach.[148] Determining the exact variant of ransomware one is dealing with can be close to impossible; malware data analysis has found and evaluated over a million unique variants of ransomware.[149] In essence, if the variant in question does not exfiltrate data, covered entities might instead chose not to report it because no data has actually been lost.[150]

Finally, a successful attack might require a covered entity to pay the ransom in order to protect the health and safety of patients. Current policy opens up covered entities to financial penalties under HIPAA whenever there is a breach, regardless of whether or not the covered entity pays the ransom or not, and so does not properly act as a deterrent for payment nor provide incentive to upgrade a covered entity's cybersecurity.[151] While the financial penalties alone provide incentive for covered entities to comply with HIPAA in ordinary circumstances,

---

146. 45 C.F.R. § 164.402(2).
147. U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 82.
148. HIPAA J., *supra* note 85.
149. Mellen, *supra* note 7.
150. *Id.*
151. *See generally*; HIPAA J., *supra* note 85.

ransomware is far from ordinary; the fact that lives are potentially at stake, in conjunction with the knowledge that a penalty is likely forthcoming regardless of whether or not the covered entity does in fact pay, must be taken into account when a covered entity succumbs to the pressure to pay for the return of its information.[152]

These outcomes serve to render the current guidelines set by HHS wholly inadequate. The guidelines must be changed if ransomware attacks are to be mitigated or stopped outright. The solution to the problems imposed by ransomware must take into account both the technical laxness of covered entities, the problems with current HIPAA legislation in regards to ransomware, and the necessity by covered entities to ensure that they are able to meet the needs of their patients.

C. Solutions to Better Deal With Ransomware

1. Solution 1: Draft New Legislation That Directly Addresses Ransomware

Even though HHS has now provided key guidance in how covered entities should approach ransomware attacks, it has also created a cumbersome, subjective, and fact-specific determination that does not incentivize covered entities to report attacks.[153] Congressmen have already acknowledged that ransomware does not fit into the typical definition of a breach.[154] Congressman Ted Lieu summed up the paradoxical nature of combating ransomware in an open letter to HHS, stating:

> However, just because a ransomware attack qualifies as a conventional breach, that does not mean they should be treated the same or subject to the exact same risk assessment . . . in a normal breach, personal health information is either viewed or stolen, infringing the privacy rights of the patient. Ransomware, however, denies access to health records or information technology functions that enable the provider to offer health care services.[155]

Any future legislation must deal with the unusual paradox posed by ransomware. Therefore, the most immediate solution to dealing with the fact-specific ambiguity of whether a ransomware attack constitutes a breach of PHI or not is to pass new or updated legislation explicitly making ransomware, regardless of the outcome or facts, to be a reportable *event* rather than a normal HIPAA breach.

In essence, while ransomware attacks would still have to be reported by covered entities when they occur, they would not automatically open up said entity to financial penalties under HIPAA, and if necessary the disclosure could be private, so as not to alert potential attackers from making additional attempts.

---

152. Snell, *supra* note 67.

153. U.S. DEP'T. OF HEALTH & HUMAN SERVS., *supra* note 4.

154. Lieu, *supra* note 68.

155. *Id.*

Such a law would have to strike a careful balance between the interest of patients in ensuring that their data has been secured and the interest of covered entities in ensuring that they are not unduly penalized for ransomware attacks.[156]

HHS should still have the power to levy fines against egregious failures to comply with HIPAA security rules, but that would be the exception and not the rule for reporting ransomware. Fines should only be levied when a covered entity has egregiously failed to protect its electronic PHI by not properly upgrading their cybersecurity or as a result of catastrophic human error. This would encourage reporting among covered entities and give agencies such as the FBI or the DHS a clearer picture of how widespread the threat of ransomware is. There has already been a strong push in Congress to pass sweeping healthcare cybersecurity legislation as more and more cyberattacks have occurred over the year.[157] By separating ransomware and its ilk into its own class of cyberattack, Congress can make it far more palatable for covered entities to report attacks.

2. Solution 2: Empower HHS To Explicitly Deal With Ransomware

As noted above, Congress has had difficulty passing cybersecurity legislation because many of its members have difficulty understanding the complexities of the cyber-world.[158] A simple way to avoid any undue delay in protecting critical cyber-infrastructure would be for Congress to further empower HHS to deal with cybersecurity requirements, delegating some of their legislative power to that effect. HHS already has a Cybersecurity Task Force in place to work with DHS and National Institutes of Science and Technology to analyze and review the threats facing the healthcare industry and strategies other industries have implemented to deter attacks.[159] However, afterwards, the Task Force only reports their findings to the Secretary of Health and Human Services and Congress and does not directly create regulations itself, as its mandate will end in March of 2017.[160]

With such a broad array of experts from both the public and private sectors already assembled, it would make logical sense for Congress to extend the Task Force's mandate and expand its regulatory power. While its findings would certainly assist Congress in creating legislation, by extending the mandate of the Cybersecurity Task Force and granting further regulatory power to Health and Human Services, the US government will be able to better respond to not only ransomware, but to current and future cybersecurity threats that could threaten the healthcare system.

Current Congressional legislative attempts to curb ransomware may fail to account for the exponential growth and threat ransomware can pose, and ransomware is constantly evolving, which may thwart current congressional efforts in unexpected ways.[161] Members of DHS have already estimated that

---

156. HIPAA J., *supra* note 85.

157. Raths, *supra* note 128.

158. *Id.*

159. U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 132.

160. *Id.*

161. *See generally* Tom Spring, *Meet the Cryptoworm, the Future of Ransomware*,

ransomware could soon start to threaten patient medical devices.[162] For legislation and regulations to keep up with the pace of cyberthreats, it is necessary for Congress to establish a permanent Cybersecurity Task Force and grant it regulatory power.

3. Solution 3: Create Financial Incentives for Covered Entities to Better Secure Their Data

The other side of this coin is ensuring that covered entities have better cybersecurity functions, so as to either thwart attacks or present such an unprofitable target as to deter future attackers. To best ensure such an outcome, Congress could help by providing financial incentives to covered entities to update and upgrade their cybersecurity systems. Congress has used similar means in the past to provide incentive for the healthcare industry to adopt new technologies; the HITECH Act, for example, provided financial incentives to encourage the adoption of electronic health records (EHR).[163] For hitting certain benchmarks in its usage of electronic health records, the government provided incentive payments to hospitals and other healthcare entities in the form of increased funding to Medicaid programs; as the program continued to grow, the government later began to levy financial penalties on hospitals and other healthcare systems that were not following suit with the early adopters.[164] HHS has reported that it has seen a significant increase in the adoption and use of health IT systems among providers and the new data shows the importance of incentives in building an interoperable health IT system.[165] These incentives have also led to widespread adoption of electronic health records across the United States, and HHS has further noted that "[S]ince the enactment of HITECH in 2009, 62 percent of physicians who adopted health IT tools identified financial incentives and penalties as a major influence on their decision to adopt, compared

---

THREATPOST (Apr. 12, 2016), https://threatpost.com/meet-the-cryptoworm-the-future-of-ransomware/117330/ (discussing the potential next threat ransomware may take in 2017) [https://perma.cc/A8CF-TKX7].

162. Greg Slabodkin, *supra* note 24.

163. *Financial incentives and ability to exchange clinical information found to be top reasons for EHR adoption*, U.S. DEP'T. OF HEALTH & HUMAN SERVS. (Dec. 5, 2014), https://wayback.archive-it.org/3926/20170128122615/https://www.hhs.gov/about/news/2014/12/05/financial-incentives-and-ability-exchange-clinical-information-found-be-top-reasons-for-ehr-adoption [https://perma.cc/ZB4V-6ZCS].

164. *Electronic Health Records (EHR) Incentive Programs*, CENTERS FOR MEDICARE & MEDICAID SERVS. (last modified Feb. 8, 2017), https://wayback.archive-it.org/3926/20170127160700/https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms [https://perma.cc/9M9X-V6GL].

165. *Financial incentives and ability to exchange clinical information found to be top reasons for EHR adoption*, U.S. DEP'T. OF HEALTH & HUMAN SERVS. (Dec. 5, 2014), https://wayback.archive-it.org/3926/20170128122615/https://www.hhs.gov/about/news/2014/12/05/financial-incentives-and-ability-exchange-clinical-information-found-be-top-reasons-for-ehr-adoption [https://perma.cc/ZB4V-6ZCS].

with only 23 percent of physicians who adopted before 2009."[166]

The U.S. government has already taken steps to provide federally funded cybersecurity education to covered entities; in 2016, HHS invested $250,000 in creating an Information Sharing and Analysis Organization, designed to facilitate information-sharing in the healthcare and public health sectors on current cyber threats, increase general cybersecurity awareness, and begin equipping stakeholders to respond to the information they are provided.[167]

While this is a good start to better equip the healthcare sector for cyber threats, covered entities will require more incentives in order to undergo fundamental cybersecurity upgrades. Similar financial incentives to the HITECH Act, like providing increased federal funding to IT programs within covered entities, providing more funding for traditional healthcare programs such as Medicare or Medicaid, or even by providing a tax write-off for some or all of the costs incurred by entities attempting to upgrade their cybersecurity systems, combined with the fear of experiencing a ransomware attack, have a strong likelihood of pushing hospitals and other healthcare providers into truly strengthening their cybersecurity systems.

III. CONCLUSION

Ransomware presents an unusually paradoxical threat to the United States' healthcare industry. While it does not seize data in the traditional manner that cybersecurity threats have typically gone after electronic PHI, it has found a new way to hurt patient safety and care by restricting much-needed access to those files. A focus on HIPAA compliance, rather than cutting-edge cybersecurity, has left the healthcare industry critically exposed to the dangers wrought by ransomware attacks.

However, as devastating as ransomware attacks have been to the healthcare industry over the past two years, they have also brought a much-needed spotlight to the threat ransomware and other cybersecurity threats pose to both the protection of patient health information and the healthcare infrastructure of the United States. Fundamental change is going to be required if we are to protect our health information.

The guidance issued by HHS offers a solid stopgap measure and a foundation for change, but it is not enough. Ransomware attacks on the healthcare industry will markedly decrease only when legislation that mandates ransomware as a reportable event while simultaneously providing financial incentives for hospitals

166. *Id.*

167. Akanksha Jayanthi, *HHS to fund cybersecurity information sharing organization*, HEALTH IT & CIO REVIEW (July 26, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/hhs-to-fund-cybersecurity-information-sharing-organization.html[https://perma.cc/NS96-SMJZ].

to improve their cybersecurity suites. It will take some time for these changes to be implemented, but the sooner Congress takes action, the sooner the dreaded specter of ransomware will cease to be a critical threat to the health infrastructure of the United States.