Hofstra Law Review

Volume 51 | Issue 4 Article 9

6-1-2023

Hacking Healthcare: Ransomware as a Rising Contagion

Elizabeth Stachtiaris
Maurice A. Deane School of Law at Hofstra University

NOTE
HACKING HEALTHCARE: RANSOMWARE AS A RISING CONTAGION

I. INTRODUCTION

During the recovery phase of the SARS-CoV-2 pandemic peak, which created its own novel challenges for hospitals and healthcare workers nationwide, a Brooklyn hospital found itself victim to a different type of virus.[1] Wyckoff Heights Medical Center ("Wyckoff"), a teaching hospital dedicated to serving the inner-city community, succumbed to ransomware of its electronic network, which put Protected Health Information ("PHI") at risk of exposure and hindered pending patient care.[2] Healthcare workers engaged in direct patient care felt flustered, frustrated, and near-helpless as they attempted to work around the malware with pen and paper, unable to access the hospital's Electronic Health Record ("EHR") until the hospital paid the ransom to the hackers.[3] While hand-written charting was once the norm of medical practice, it is now archaic and even an impediment.[4] In the era of hand-written charting, physicians and nurses were unable to log into the hospital network or EHR, review patients' prior medical records, or efficiently order or analyze tests, such as lab work or imaging.[5] But even when a healthcare organization is functioning properly, a myriad of human medical errors result in poor patient outcomes and deaths.[6] The

1. Kapua Iao, *Wyckoff Heights Medical Center Struck by Ransomware*, PAUBOX (Dec. 8, 2020), https://www.paubox.com/blog/wyckoff-heights-medical-center-struck-ransomware [https://perma.cc/WJQ6-RRM9].

2. *Id.*

3. *Id.*

4. *See Advantages and Disadvantages of Paper Medical Records*, TRUENORTH, https://www.truenorthitg.com/pros-and-cons-paper-medical-records [https://perma.cc/UVK3-4BBB] (last visited Aug. 12, 2023).

5. E-mail from Tiffany Fieldings, Physician, Wyckoff Heights Medical Ctr., to Elizabeth Stachtiaris, Physician, Brookdale Hospital Medical Ctr. (Sept. 28, 2021, 10:42 AM) (on file with author) [hereinafter Fieldings E-mail].

6. *See* INSTITUTE OF MEDICINE, TO ERR IS HUMAN: BUILDING A BETTER HEALTH SYSTEM 26 (Linda T. Kohn et al. eds., 2000) (elucidating that medical errors made by healthcare workers account for up to 98,000 deaths per year, outnumbering deaths caused by several intrinsic pathological illnesses).

withholding by ransomware of a vital tool of modern medicine on which clinicians rely exponentially increases the risk of medical errors, poor patient health outcomes, and physician liability for medical malpractice.[7]

While Wyckoff did not ultimately need to divert patients to other nearby hospitals and instead utilized a backup system of paper charting for several weeks,[8] many hospitals nationwide that experienced similar malware attacks did divert patients, such as MedStar in Washington, D.C., after the ransom devastated most of its institutional system in 2016.[9] More recently, a Missouri hospital's EHR was breached not for the purpose of denying access to caregivers, but to expose PHI by obtaining and posting patients' sensitive information online.[10] These attacks are not occurring sporadically or in isolation, but frequently and at multiple healthcare institutions simultaneously.[11] The aforementioned incidents are merely a few of thousands of attacks, providing a snippet of this novel and ironic epidemic of infectious ransomware.[12]

Since the late twentieth century with the innovations of electronics and the internet, a niche was inadvertently created for hackers to infiltrate devices for profit.[13] Medicine, an inherently high-stakes field which literally and directly involves the well-being of individuals, was forced to embrace a new epoch of EHR, if not for the mainstream sharing of PHI among mutual providers, then for streamlined billing purposes.[14] Ransomware is an apparent and increasing threat to

---

7. Babur Kahn, *Death by Ransomware: Poor Healthcare Cybersecurity*, HIT CONSULTANT (Jan. 5, 2021), https://hitconsultant.net/2021/01/05/death-by-ransomware-healthcare-cybersecurity/#.YUewxWZKhpU [https://perma.cc/WG7Y-8MM7].

8. Fieldings E-mail, *supra* note 5.

9. John W. 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/49MM-39A8].

10. Jackie Drees, *Ransomware Group Targets Missouri Hospital, Posts Patients' Info Online*, BECKER'S HOSP. REV. (Sept. 17, 2021), https://www.beckershospitalreview.com/cybersecurity/ransomware-group-targets-missouri-hospital-posts-patients-info-online.html [https://perma.cc/6Q3G-WK33].

11. *See generally Health IT*, BECKER'S HOSP. REV., https://www.beckershospitalreview.com/healthcare-information-technology [https://perma.cc/RH5W-VQFH] (last visited Aug. 12, 2023) (detailing the alarming frequency of cybersecurity breaches targeting hospitals that result in PHI exfiltration and/or blocked EHR access to providers).

12. *Id.*

13. LastWeekTonight, *Ransomware: Last Week Tonight with John Oliver (HBO)*, YOUTUBE (Aug. 16, 2021), https://www.youtube.com/watch?v=WqD-ATqw3js [https://perma.cc/HN3K-27MX] (detailing the history and development of ransomware, including its inner machinations, progression from early crude to refined models, span from personal infiltrations to large-scale attacks, and potential significant monetary gains within the malware industry).

14. *See infra* Part II.C.

healthcare institutions with attacks rising rapidly, a danger that was unfathomable in the era of paper medical records.[15] Hackers are targeting healthcare facilities due to the widespread dearth of network and cybersecurity measures, which vary institutionally and are sometimes minimally existent.[16] For a field that has transitioned from bedside to desktop,[17] medical cybersecurity has not appropriately followed.[18]

Healthcare was jettisoned, in some cases forcibly, into the technological age via the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which, as written, incentivizes all healthcare facilities to convert all paper charting to EHR, presumably for ultimately improved patient outcomes.[19] However, the "incentive" for converting to EHR was essentially a mandate, demanding uniformity to abandon paper and embrace Health Information Technology ("HIT").[20] Naturally, all HIT would have to comply with the Health Information Portability and Accountability Act ("HIPAA"), which demands ensuring the privacy of patient PHI in all media.[21] Furthermore, neither HITECH nor HIPAA address network security; rather, the former solely mentions EHR and EHR security.[22] The subtle, yet important, difference between network and EHR is omitted from the aforementioned Acts, likely because the two are so interwoven, yet are separate entities requiring unique security measures.[23] Notwithstanding these Acts' disregard for this nuance, they nevertheless render the healthcare industry vulnerable to security breaches on both fronts as neither outlines sufficient safeguards against cyberthreats.[24] While ransomware threatens the

15. Iao, *supra* note 1.

16. Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE U.L. REV. 937, 941 (2017).

17. Pauline W. Chen, *The Rise of Desktop Medicine*, N.Y. TIMES (Mar. 31, 2011, 11:28 AM), https://well.blogs.nytimes.com/2011/03/31/the-rise-of-desktop-medicine [https://perma.cc/2J8E-GTWV].

18. *See* Farringer, *supra* note 16, at 941.

19. *See* The Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 13001–14002.

20. Farringer, *supra* note 16, at 944, 946.

21. *See* Health Information Portability and Accountability Act, Pub. Law No. 104-191, § 1177, 110 Stat. 1936, 2029 (1996).

22. *See generally* 42 U.S.C. §§ 17901–17903 (2009) (codifying the incentivization of transitioning all healthcare facilities' charting systems to EHR and mentioning EHR security).

23. May Elliot, *Information Security vs Cybersecurity vs Network Security: Are They the Same?*, NEWCLOUD (Jan. 23, 2020, 11:00 AM), https://web.archive.org/web/20200813141010/https://blog.newcloudnetworks.com/information-security-vs-cybersecurity-vs-network-security-are-they-the-same [https://perma.cc/598P-2D7S?type=image].

24. Farringer, *supra* note 16, at 941.

exfiltration of PHI,[25] which contains records of past patient care, its more hazardous and immediate effect is blocking clinician access to EHR, detrimentally impacting present and future patient care and outcomes.[26]

This Note delineates the gravity of ransomware in the context of HIT and how it severely debilitates a provider's ability to deliver care to patients as well as the risk of exposure of PHI.[27] It elucidates that, while HIPAA and HITECH were enacted to streamline the technicalities of medicine, they ironically leave healthcare facilities vulnerable to this novel malware, which did not exist during the time of the Acts' drafting.[28] In order to combat this threat to PHI and clinician ability to render care, both HIPAA and HITECH must be amended with the risk of ransomware at the forefront, prescribing at least a minimum standard of network and cybersecurity, with which all healthcare facilities must comply.[29] Part II of this Note details the practice of medicine: both traditionally and as it shifts more from the patient's bedside to the computer.[30] It explores the implementation of HIT and, with it, the rise and development of the ransomware industry.[31] It also illuminates the crucial distinction between network and the internet, as well as their counterparts network security and cybersecurity, respectively.[32] Additionally, it introduces and illustrates HIPAA and HITECH.[33] Part III questions these Acts, exposing their shortcomings and how they paved the way for the current state of ransomware attacks targeting healthcare institutions, jeopardizing both past and present patient care.[34] Part IV proposes innovative solutions for the aforementioned legal issues, explicitly detailing certain minimum standards of network and cybersecurity to be implemented in amendments to both HIPAA and HITECH.[35] Finally, Part V concludes this Note by summarizing the aforementioned Parts and optimistically imploring Congress to adopt these proposed solutions to this grave and growing legal dilemma.[36]

---

25. Ranjit Janardhanan, *Uncle Sam Knows What's in Your Medicine Cabinet: The Security and Privacy Protection of Health Records Under the HITECH Act*, 30 J. MARSHALL J. INFO. TECH. & PRIV. L. 667, 668 (2014).

26. Cox, *supra* note 9.

27. *See infra* Part II.

28. *See infra* Part III.

29. *See infra* Part IV.

30. *See infra* Part II.A–C.

31. *See infra* Part II.C, II.F.

32. *See infra* Part II.D–E.

33. *See infra* Part II.G–H.

34. *See infra* Part III.

35. *See infra* Part IV.

36. *See infra* Part V.

II. BACKGROUND

In order to fully comprehend the extent to which HIT, and its susceptibility to ransomware, has been incorporated into medical practice, a thorough elucidation of the physician-patient interaction during the latest decades of technological innovation is necessary.[37] In addition to a history of the emergence of technomedicine with the main focus on the distinction between a hospital's network and EHR, it is also vital to discuss the legal framework that governs PHI and HIT.[38] Part II.A of this Note details the physician-patient encounter prior to EHR along with the benefits and shortcomings of paper charting.[39] Part II.B tales the rise of technomedicine, not only regarding EHR, but medical devices generally and how they influence current medical practice.[40] Part II.C specifically discusses EHR: its development, utilization, pros, and cons.[41] Part II.D describes the subtle, yet important, distinction between network and cyber as well as their respective implementable security measures.[42] Parts II.E and II.F explain the origins of ransomware, first in the context of general electronics and then more narrowly in the genre of medicine and EHR.[43] Parts II.G and II.H introduce legislation and statutes, namely HIPAA, HITECH, and their effects on medical practice.[44] Part II.I draws a brief overview of the Emergency Medical Treatment and Labor Act ("EMTALA") and how it affects emergency medical practice.[45]

A. Traditional Practice of Medicine

Contrary to laymen's belief, the majority of a physician's time is not spent at the bedside, but is rather dedicated to charting, placing orders, and analyzing test results.[46] This practice existed even before technology pervaded medicine,[47] likely because of the adage, "If you didn't document it, it never happened," aimed to prophylactically avoid

37. *See infra* Part II.
38. *See infra* Part II.
39. *See infra* Part II.A.
40. *See infra* Part II.B.
41. *See infra* Part II.C.
42. *See infra* Part II.D.
43. *See infra* Part II.E–F.
44. *See infra* Part II.G–H.
45. *See infra* Part II.I.
46. *See* Stephanie Desmon et al., *Doctors-In-Training Spend Very Little Time at Patient Bedside, Study Finds*, JOHNS HOPKINS MED. (Apr. 23, 2013), https://www.hopkinsmedicine.org/news/media/releases/doctors_in_training_spend_very_little_time_at_patient_bedside_study_finds [https://perma.cc/32HF-4329].
47. *Id.*

malpractice suits.[48] However, although doctors spent more time documenting than with the patient, the former was significantly less when paper charts were utilized.[49] The transition to desktop medicine has left fledgling physicians without honed clinical skills, such as percussion,[50] opting for technomedicine with less inter-clinician variability.[51] Traditionally, paper charts consisted of a "T-sheet," which invited brief check marks to an objective section on an anachronistic template.[52] However, the subjective section of the "T-sheet" required physicians to handwrite the history of present illness, and often suffered from illegibility, potentially leading to medical errors.[53] Diagnoses relied on physical exam findings prior to the innovation of radiography, after which it blended into routine patient care.[54] Furthermore, with merely one copy of each chart residing on the same unit as the patient, paper charts lacked convenient accessibility, forcing consultants to search for and find the sometimes-elusive chart in order to contribute recommendations.[55] The contents within were insecure since there was no method to log who viewed the notes, as opposed to EHR, which keeps track of each user who enters the chart.[56] More generally, the entire chart itself was insecure as there were likely no duplicates after disasters, such as fire or flood.[57]

---

48. Mark Bassingthwaighte, *When It Comes to Malpractice Claims, If You Didn't Document It, It Never Happened*, 43 MONT. L., Oct. 2017, at 27.

49. *See* Desmon et al., *supra* note 46.

50. Melinda Henry & Jamie Newman, *The Birth of Percussion*, HOSPITALIST (Apr. 1, 2006), https://www.the-hospitalist.org/hospitalist/article/123104/birth-percussion [https://perma.cc/8UEG-G6JR] (defining "percussion" as a physician's tapping on the chest wall or abdomen to elicit certain sounds that indicate pathology, such as if the lungs are filled with fluid or if hepatosplenomegaly is present, and elucidating the practice of percussion, including its origin, purpose, and history throughout medicine as it fades and is replaced by radiography and serum testing).

51. Anna Harris, *Listening-Touch, Affect and the Crafting of Medical Bodies Through Percussion*, BODY & SOC., Mar. 2016, at 31, 33.

52. Rick Weinhaus, *EHR Design Talk with Dr. Rick*, HISTALK: HEALTHCARE IT NEWS & OP. (Feb. 6, 2012), https://histalk2.com/2012/02/06/ehr-design-talk-with-dr-rick-2612 [https://perma.cc/5HNV-3Z8E].

53. Jeremy Caplan, *Cause of Death: Sloppy Doctors*, TIME (Jan. 15, 2007), http://content.time.com/time/health/article/0,8599,1578074,00.html [https://perma.cc/BZ2X-R93B] (discussing the disturbing amount of medical errors and patient deaths caused by physicians' illegible handwriting and endorsing EHR as a solution that should be uniformly adopted by all healthcare professionals); *see also For All Who Hate Computers in Medicine: Here's What We Got Before*, E-PATIENT DAVE: DEMOCRATIZING HEALTHCARE (Jan. 27, 2020), https://www.epatientdave.com/2020/01/07/for-all-who-hate-computers-in-medicine-heres-what-we-got-before [https://perma.cc/VCK5-7Y8A].

54. Joel Howell, *Early Clinical Use of the X-Ray*, 127 TRANSACTIONS AM. CLINICAL & CLIMATOLOGICAL ASSOC. 341, 346 (2016).

55. *Advantages and Disadvantages of Paper Medical Records*, *supra* note 4.

56. *Id.*

57. *Id.*

B. Evolution from Paper to Electronic

During the twentieth century, technological advances inundated every aspect of life, including healthcare, which enhanced, and sometimes altered, medical practice.[58] Whether or not this was spurred by ulterior motives of economics and profit under the guise of improving patient care, the time came for healthcare professionals to "embrace 'the future' as it has become the present."[59] Obvious improvements include the elimination of illegible handwriting, greater accessibility from any unit or even remotely from home, and ease of research tracking.[60] Medical technology does not solely refer to the EHR upon which the physician orders tests and documents patient encounters, but also refers to radiography, cardiac monitors, pacemakers, and more.[61] Wireless devices improve portability and efficiency, especially when brought to the patient's bedside and implemented during the history of present illness in real time.[62] Additionally, the adoption of devices and EHR theoretically reduces human medical errors.[63] The exponential growth of technomedicine has created a reliance upon electronics by both patient and physician.[64] Regardless of using paper charts versus EHR, a patient's case cannot progress without the physician leaving the bedside to place orders and subsequently analyze the test results.[65]

C. The Development of and Subsequent Reliance upon EHR

Primitive EHR was birthed in the mid-1960s and termed "clinical information systems," an ancestor of the current EHR system known as Allscripts.[66] The federal government adopted EHR first in the 1970s for

58. Rilind Elezaj, *How Technology Has Changed the World of Medicine*, GEOSPATIAL WORLD (Oct. 22, 2018), https://www.geospatialworld.net/blogs/how-technology-has-changed-the-world-of-medicine [https://perma.cc/65XE-WKJN].

59. Jim Atherton, *Development of the Electronic Health Record*, 13 AMA J. ETHICS 186, 186 (2011).

60. *Id.*; *see also* E-mail from Conrad Fischer, Physician, Brookdale Hospital Medical Ctr., to Elizabeth Stachtiaris, Physician, Brookdale Hospital Medical Ctr. (Nov. 8, 2021, 5:29 PM) (on file with author) [hereinafter Fischer E-mail] (illustrating the inconvenience of having to write emergent consult notes during the era of paper charts, when the only access to the paper record was within the hospital on the same unit as the patient, forcing all consultants to be physically present to contribute notes and recommendations).

61. *See* Elezaj, *supra* note 58.

62. *Id.*

63. Edward Ambinder, *A History of the Shift Toward Full Computerization of Medicine*, 1 JCO ONCOLOGY PRAC. 54, 54 (2005).

64. Chen, *supra* note 17.

65. Desmon et al., *supra* note 46.

66. Atherton, *supra* note 59, at 187.

utilization with the Veteran Affairs system.[67] An early benefit of the new EHR systems was accessibility, allowing multiple users simultaneously to access and contribute to a patient's chart.[68] As its development became more robust, it also allowed for a mainstreamed billing system, which resulted in higher and more efficient reimbursements to healthcare facilities.[69] Additionally, EHR offered security measures unattainable in hard copy format, including the log history of which user viewed certain charts, as well as data storage systems that ensured chart recovery should an external catastrophe manifest.[70] During the 1980s, the use of EHR was promulgated as a method to improve medical practice efficiency and also decrease errors.[71] However, implementation across small medical practices and hospitals remained sporadic as there was little incentive for clinics, especially solo practitioners, to invest such a large sum into converting paper records to EHR.[72] Indeed, adoption of EHR was a slow trend, progressing throughout the early decades of the 2000s.[73]

While EHR is more efficient and less cumbersome than paper charts, it possesses its own inherent issues.[74] EHR is mostly utilized on the immobile desktop, forcing physicians to retreat to the charting station and remain there rather than the patient's bedside to place orders and document.[75] This is a large part of the reason why time at the bedside has decreased.[76] This issue can be circumvented by the use of Computers on Wheels ("COW") or Workstations on Wheels ("WOW"); however, this conspicuously adds a large physical barrier between

67. *Id.* (elucidating that the initial implementation of EHR by the federal government was within the Veterans Affairs system). The Veterans Affairs system provides health and medical services to veterans for little-to-no cost. *Veterans Health Administration*, U.S. DEP'T OF VETERANS AFFS. (Sept. 28, 2021), https://www.va.gov/health [https://perma.cc/3ZTH-FNAF].

68. Atherton, *supra* note 59, at 187.

69. *See* INSTITUTE OF MEDICINE, THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE 119 (Richard S. Dick et al. eds., rev. ed. 1997).

70. *Advantages and Disadvantages of Paper Medical Records*, *supra* note 4.

71. INSTITUTE OF MEDICINE, *supra* note 69, at 119.

72. Nir Menachemi et al., *Benefits and Drawbacks of Electronic Health Record Systems*, 4 RISK MGMT. & HEALTHCARE POL'Y 47, 51 (2011).

73. JaWanna Henry et al., *Adoption of Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals: 2008-2015*, 35 ONC DATA BRIEF, May 2016, at 1, https://www.healthit.gov/data/data-briefs/adoption-electronic-health-record-systems-among-us-non-federal-acute-care-1 [https://perma.cc/E368-B249].

74. *See* Peter Rippey, *Eye on the Ball: Overreliance on EHRs Can Bring Disaster*, AAFP NEWS BLOG (Sept. 21, 2015), https://web.archive.org/web/20210802001750/https://www.aafp.org/news/blogs/freshperspective [https://perma.cc/F8RN-R2HU].

75. Chen, *supra* note 17.

76. Desmon et al., *supra* note 46.

face-to-face physician-patient interaction.[77] Furthermore, EHR creates an overuse of prepopulated templates, likely a surreptitious motive of billers ensuring that the physician documents at least the minimum amount of organ systems to bill for a certain level of service in order to maximize reimbursements.[78] Such templates may lead to dependence on electronic communications and decreased interpersonal communication in real time, potentially resulting in poor patient outcomes in emergency situations.[79]

As with many technological advances generally in society, the synergistic relationship becomes almost parasitic as an innate reliance is formed.[80] This occurs more seriously with younger physicians who have only practiced during the dynasty of EHR, whereas more senior doctors are able to utilize paper charts more easily since this is how they were initially trained.[81] Some EHRs are almost too user-friendly, auto-populating medication dosages, and not requiring the prescriber to commit such details to memory.[82] However, regardless of varying physician training, it is undeniable that even if T-sheets are easier for some clinicians, the hospital's throughput cannot rely on their efficiency for one user; rather, the institution as a whole must function within and across different departments, demanding one cohesive system.[83] Even without malfunctions within the EHR or facility network, a clinician may need to resort to backup measures of functioning without these tools.[84] Many hospitals experience both scheduled and unscheduled "downtime," during which backup procedures must be undertaken, usually in the form of paper charting.[85] "Scheduled downtime" is preceded by a warning to all clinical staff members when updates to the

77. Deborah Whittemore et al., *COWs and WOWs, Oh My!*, HEALTHCARE INNOVATION (July 1, 2008), https://www.hcinnovationgroup.com/home/article/13000590/cows-and-wows-oh-my [https://perma.cc/R6JF-KUBY?type=standard].

78. *Extra Care Needed in Use of Prepopulated EHR Templates*, ACOI, https://web.archive.org/web/20220528125620/https://www.acoi.org/coding/extra-care-needed-use-prepopulated-ehr-templates [https://perma.cc/9S6K-EDYA?type=standard] (last visited Aug. 12, 2023).

79. Rippey, *supra* note 74.

80. Terry Brown, *Are We Too Dependent on Technology?*, ITCHRONICLES (Mar. 31, 2020), https://itchronicles.com/technology/are-we-too-dependent-on-technology [https://perma.cc/72G7-2HTL].

81. Fieldings E-mail, *supra* note 5.

82. Rippey, *supra* note 74.

83. Fieldings E-mail, *supra* note 5.

84. Tracy Dowlat, *EPIC Downtime*, ONE BROOK. HEALTH–BROOKDALE HOSP. MED. CTR., June 2021, at 1 (on file with One Brooklyn Health–Brookdale Hospital Medical Center) (describing the hospital protocol that all staff members and clinicians must follow when the EHR is unavailable, mainly reverting to paper orders and documentation).

85. *See, e.g.*, *id.*

software are planned and the system cannot be utilized and usually takes place during early morning hours when patient volume is presumed to be lower.[86] "Unscheduled downtime" is typically unexpected and may be caused by a malicious breach.[87] Whether scheduled or unscheduled, downtime and paper charting create a significant inconvenience to providers and staff mainly due to their reliance upon the user-friendly EHR,[88] which can indirectly affect patient care, especially when information gets lost amongst the paper piles.[89]

D. The Difference Between Network, EHR, and Cyber/Internet

In order to fully grasp the nuances of HIT, a brief differentiation of all of its aspects is necessary.[90] Starting with the basics, HIT is the processing, storage, and exchange of health information in electronic form.[91] Its implementation into healthcare was aimed to increase efficiency and quality of care delivered while also decreasing medical errors and cost.[92] HIT includes numerous devices that have been incorporated into healthcare and have subsequently become inherent in the practice of medicine, such as X-Ray machines, CT scanners, desktops, laptops, and even cellular phones.[93]

All HIT devices must communicate with each other in order to be effective in the delivery of healthcare and thus rely on a local network.[94] The network of each healthcare facility encompasses all institutional HIT devices and the connection between them.[95] This includes not only the aforementioned technology, but also the server and intranet[96] that

86. *Id.* at 5.

87. *Emergency Preparedness: Be Ready for Unanticipated Electronic Health Record (EHR) Downtime*, INST. FOR SAFE MEDICATION PRACS. (Aug. 25, 2022), https://www.ismp.org/resources/emergency-preparedness-be-ready-unanticipated-electronic-health-record-ehr-downtime [https://perma.cc/6K27-UTTK]. *See generally* Fieldings E-mail, *supra* note 5 (detailing a physician's perspective of the difficulty working during unscheduled downtime due to malware).

88. Rippey, *supra* note 74.

89. Fieldings E-mail, *supra* note 5.

90. E-mail from William Ahrens, Director, Mazars USA, to Elizabeth Stachtiaris, Physician, Brookdale Hospital Medical Ctr. (Sept. 27, 2021, 8:19 AM) (on file with author) [hereinafter Ahrens E-mail].

91. *Health Information Technology*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html [https://perma.cc/37QA-KHWU] (last visited Aug. 12, 2023).

92. *Id.*

93. Ahrens E-mail, *supra* note 90.

94. *Id.*

95. *Id.*

96. E-mail from Sandra Scott, Exec. Dir., One Brooklyn Health, to Cynthia Bui, Asst. Medical Dir. of Emergency Medicine, One Brooklyn Health (Nov. 4, 2021, 4:23 PM) (on file with

allows them to interact.[97] Another way to imagine this connection is the "cloud."[98] The HIT devices, local network, server, and intranet are entirely unique to each institution and designated as "inside" hardware and software.[99] For example, when a radiograph is performed, the image is stored on the X-Ray machine itself and then subsequently uploaded to the cloud.[100] From there it is transmitted via the network and intranet to the computer, where the physician can access and view it, usually on a software system such as the Picture Archiving and Communication System ("PACS").[101] Before HIT, radiology consisted of shooting an X-Ray film, developing the single copy manually, delivering the film to the in-house radiologist to interpret, and the radiologist delivering his findings verbally or via handwritten note.[102] After integrating EHR and HIT into radiography, the whole system of ordering radiographic studies, accessibility to radiologists, and delivery to clinicians improved ease and efficiency, and therefore, patient care.[103] Similarly, another example of HIT connections is the printer system, which is linked wirelessly to the desktops of the institution via the network.[104] These connections between hardware and software of the health institution allow HIT to synergistically combine to allow more efficient delivery of healthcare to patients.[105]

EHR is another type of HIT in the form of software that was created to replace the archaic handwritten charting system, improve efficiency, and decrease medical errors.[106] EHR is the digitized form of a patient's chart, which contains medical history, diagnoses, test results, medication history, and plans for future care.[107] Early prototypes

---

author) [hereinafter Scott E-mail] (clarifying that the intranet is not a website, but a "SharePoint database" accessible within the One Brooklyn Health system facilities).

97. Ahrens E-mail, *supra* note 90.

98. *Health Information Technology*, *supra* note 91.

99. Ahrens E-mail, *supra* note 90.

100. *Id.*

101. *Id.*; *Picture Archiving and Communication System*, EHEALTH SASKATCHEWAN, https://www.ehealthsask.ca/services/PACS [https://perma.cc/QTN7-BQLV?type=standard] (last visited Aug. 12, 2023).

102. *From Films to Digital, The Evolution of Imaging Records*, JOHNS HOPKINS MED. (Jan. 21, 2022), https://www.hopkinsmedicine.org/news/articles/from-films-to-digital-the-evolution-of-imaging-records [https://perma.cc/HEV3-XPAA].

103. Benjamin Wildman-Tobriner et al., *Moving Radiology Workflow to the Electronic Health Record: Quantitative and Qualitative Experience from a Large Academic Medical Center*, 27 ACAD. RADIOLOGY 253, 253-55 (2020).

104. Ahrens E-mail, *supra* note 90.

105. *Health Information Technology*, *supra* note 91.

106. Caplan, *supra* note 53.

107. *What Is an Electronic Health Record (EHR)?*, HEALTHIT.GOV, https://www.healthit.gov/faq/what-electronic-health-record-ehr [https://perma.cc/V4TG-CHGQ] (last visited Aug. 12, 2023).

emerged in the 1960s with the federal government adopting its utilization in the 1970s.[108] Instead of a folder filled with handwritten paper, documentation, and test results with only a single available copy, EHR replaced this cumbersome and inconvenient file with a computer program, installed onto a hospital's network, and therefore connected to other devices in a similar fashion via the intranet.[109] The notoriously poor handwriting of physicians was replaced by universally legible typeface,[110] and any patient's medical chart was accessible from any computer connected to the network, thus increasing accessibility.[111] The EHR allowed a clinician to document patient encounters, order tests, receive results of said tests, and access other EHR-compatible software, such as PACS, to directly visualize radiographs, analyze, and interpret them.[112] This workflow resulted in decreased length of stays, fewer delays of care, and less unnecessary duplicate testing.[113] EHR also implemented best practice advisories and evidence-based clinical decision tools, such as the HEART score for predicting major cardiac events,[114] aimed to decrease medical errors.[115] It also possessed the capabilities to track patient data over time and more easily contribute to retrospective research studies.[116] Further, EHR created a medium for e-prescribing medications directly to pharmacies, thus decreasing drug interactions due to polypharmacy and prescription fraud.[117] Just as in any capitalistic market, several competing brands of EHR exist, boasting their idiosyncratic methods to improve hospital metrics and clinician satisfaction.[118] Notable company names include EPIC, Allscripts, and Meditech.[119] However, all models of EHR must possess a baseline

108. Atherton, *supra* note 59, at 187.

109. *Electronic Health Records*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Medicare/E-Health/EHealthRecords [https://perma.cc/E4TD-3EYS] (last visited Aug. 12, 2023); *What Is an Electronic Health Record (EHR)?*, *supra* note 107.

110. *For All Who Hate Computers in Medicine: Here's What We Got Before*, *supra* note 53.

111. *See* Fischer E-mail, *supra* note 60.

112. *Electronic Health Records*, *supra* note 109.

113. *Id.*

114. *HEART Score for Major Cardiac Events*, MD+ CALC, https://www.mdcalc.com/heart-score-major-cardiac-events [https://perma.cc/8GXZ-C2BS] (last visited Aug. 12, 2023) [hereinafter *HEART Score*]. "HEART" stands for history, EKG, age, risk factors, and initial troponin. *See id.*

115. *Electronic Health Records*, *supra* note 109.

116. Martin R. Cowie et al., *Electronic Health Records to Facilitate Clinical Research*, 106 CLINICAL RSCH. CARDIOLOGY 1, 2 (2017).

117. *What Is Electronic Prescribing?*, HEALTHIT.GOV, https://www.healthit.gov/faq/what-electronic-prescribing [https://perma.cc/45RJ-67ZB] (last visited Aug. 12, 2023).

118. *Physicians Choose Their Top 10 EHR Systems for 2023*, PRAXIS, https://www.praxisemr.com/top-ehr-physicians-systems.html [https://perma.cc/N9YA-Y66H] (last visited Aug. 12, 2023) [hereinafter PRAXIS].

119. *Id.*

functionality, interoperability, usability, compliance, and performance.[120] Furthermore, they all must allow the institution to comply with federal regulations, such as HIPAA.[121] While EHR has the aforementioned advantages, its universal adoption was a slow trend, mainly due to the exorbitant cost to individual institutions to convert their paper systems, leaving smaller healthcare facilities at a disadvantage.[122] Also, the changeover to EHR did not guarantee convenient inter-hospital access to patient information by providers since there is limited interoperability between HIT systems because the main focus of the sudden shift to EHR focused merely on "providers' *use*" of the system in general.[123]

The local network of an institution must be distinguished from the internet as they remain separate entities, although admittedly as time passes and technology advances, the lines between them are blurring.[124] While the network and intranet are considered to be "inside" a facility, the internet is designated as "outside," or also known as the "cyber realm."[125] Primitive model construction of the internet began in the late 1960s and early 1970s, continuously developing and peaking in the early 2000s,[126] until, as for most modern privileged individuals, it became a ubiquitous part of life.[127] The internet itself is a large network and, just like a local network consisting of an institution's hardware, software, and how they are connected, the internet is similar on a larger scale: hardware, software, and the connection between them—except rather than remaining exclusive, it encompasses infinite devices and connections globally.[128] The internet also allows smaller networks to interact with each other.[129] Initially, an individual device required a physical wired connection to link to the internet, but as technology advanced, wireless connections were made possible via Wi-Fi and

120. Andrei Mikhailau, *EHR Testing: Specifics and Best Practices*, HEALTH IT OUTCOMES (Sept. 24, 2019), https://www.healthitoutcomes.com/doc/ehr-testing-specifics-and-best-practices-0001 [https://perma.cc/83A8-TRP2].

121. *See infra* Part III.A; *see also* Ahrens E-mail, *supra* note 90.

122. Farringer, *supra* note 16, at 946.

123. *Id.* at 947.

124. Ahrens E-mail, *supra* note 90.

125. *Id.*; pp_pankaj, *Difference Between Network Security and Cyber Security*, GEEKSFORGEEKS (June 13, 2022), https://www.geeksforgeeks.org/difference-between-network-security-and-cyber-security [https://perma.cc/4MMP-R8E4].

126. Timothy B. Lee, *The Internet, Explained*, VOX (May 14, 2015, 12:38 PM), https://www.vox.com/2014/6/16/18076282/the-internet [https://perma.cc/A6AC-MKUE].

127. Barry Wellman & Caroline Haythornthwaite, *The Internet in Everyday Life: An Introduction*, *in* THE INTERNET IN EVERYDAY LIFE 3, 4 (Barry Wellman & Caroline Haythornthwaite eds., 1st ed. 2002).

128. Lee, *supra* note 126.

129. *Id.*

cellular networks.[130] In the context of HIT, the EHR is a software program that operates on a hospital's local network amongst its local devices, which also have internet connection capabilities to myriad other devices worldwide.[131] Therefore, the lines demarcating the three are naturally blending, especially as technological innovations increase.[132]

Since the local network and the internet are vastly distinct, they carry their own distinct threats.[133] Simply, two types of technological dangers exist: those on the institution's network from within the facility itself and those from the outside cyber realm.[134] Generally, the network, as the target, is vulnerable to both sources of malware.[135] Significant threats from the cyber realm include phishing and pretexting, usually utilizing the internet to deliver an infected link, upon which an employee clicks and activates.[136] Network threats include viruses and worms, usually directly uploaded onto the network via an external device, such as a USB drive.[137] The earliest malware was propagated by floppy disk in 1989.[138] Institutions are responsible for protecting the network, commonly by the installation of anti-virus software, firewalls, and Virtual Private Networks ("VPN").[139]

E. What Is Ransomware?

Ransomware is an increasingly emerging industry, projected by the Federal Bureau of Investigation ("FBI") to gross billions of dollars in 2017.[140] Likened to "digital extortion," it began around 2005 in Eastern

130. *Id.*

131. Ahrens E-mail, *supra* note 90.

132. *Id.*

133. pp_pankaj, *supra* note 125.

134. Ahrens E-mail, *supra* note 90.

135. *Id.*

136. *Information Security vs Cybersecurity vs Network Security*, SECUREWORKS (Mar. 2, 2022), https://www.secureworks.com/blog/cybersecurity-vs-network-security-vs-information-security [https://perma.cc/T4KZ-E2GM].

137. *Id.*

138. LastWeekTonight, *supra* note 13.

139. *Information Security vs Cybersecurity vs Network Security*, *supra* note 136. The VPN is cybersecurity software that disguises one's Internet Protocol ("IP") address on a public internet connection to make it untraceable, thus increasing security and privacy. Steven Symanovich, *What is a VPN?*, NORTON (Jan. 14, 2021), https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html [https://perma.cc/QSM8-ARF4].

140. Jim Stackhouse, *Cisco and Ransomware–Anatomy of Cyber Attack*, YOUTUBE (May 16, 2017), https://www.youtube.com/watch?v=668mc-_kJBM [https://perma.cc/J7F8-Y78R] (explaining the basics of hacking and ransomware via a fictitious video reenactment, which illustrates the complex relationship of the hacker, employer, and target; and the FBI's prediction that the ransomware industry will gross one billion dollars in 2017).

Europe and continues to grow.[141] Simply, it is a heightened form of malware, targeting encryption of personal files on a device with the goal of blackmailing the owner to pay a sum to ensure their safe return.[142] The payment is typically demanded in cryptocurrency, such as Bitcoin, due to its lack of governmental regulation.[143] Classically, a hacker is paid a fee as a third party to launch the ransomware attack by an employer who targets the victim.[144] Usually, these employers originate abroad, such as in China or Russia.[145] A common method of infiltration to an institution's network by hackers is phishing, which entails luring an employee to unknowingly download malware under the guise of a seemingly trustworthy communication, such as e-mail—a commonplace contact method with devastating sequelae triggered by a simple click.[146] Ransomware is pervasive, affecting all entities from the lowly individual to wealthy conglomerates, with the goal of profit since usually the ransom price is less than the high cost of fighting the malware while risking the encrypted data.[147] The results of these attacks range from minor inconveniences to national crises,[148] such as with the case of the cyberattack on the Colonial Pipeline, causing gas runs and shortages along the United States' east coast in April 2021.[149] Traditionally, ransomware attacks surge on holiday weekends, when offices are closed

141. 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/2ANF-DRGG].

142. *Ransomware 101*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware/ransomware-101 [https://perma.cc/2EZP-LLUE] (last visited Aug. 12, 2023).

143. *What Is Ransomware?*, CISCO, https://www.cisco.com/c/en/us/solutions/security/ransomware-defense/what-is-ransomware.html [https://perma.cc/3J9U-3NQP] (last visited Aug. 12, 2023); Farringer, *supra* note 16, at 938 n.4.

144. Stackhouse, *supra* note 140.

145. Farringer, *supra* note 16, at 961.

146. *See What is Phishing?*, CISCO, https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works [https://perma.cc/SX44-DGJC] (last visited Aug. 12, 2023); *see also* E-mail from Info. Tech. Dep't., One Brooklyn Health, to All Staff, Brookdale Hospital Medical Ctr. (Dec. 18, 2021, 11:18 AM) (on file with author) [hereinafter IT E-mail] (warning employees of One Brooklyn Health system to beware of a specific phishing threat, further defining phishing as notifications that masquerade as messages from familiar contacts, and to refrain from clicking links both within the system's work e-mail as well as on each individual's personal e-mail).

147. LastWeekTonight, *supra* note 13; Ahrens E-mail, *supra* note 90.

148. Aruna Viswanatha & Dustin Volz, *FBI Director Compares Ransomware Challenge to 9/11*, WALL ST. J. (June 4, 2021, 12:56 PM), https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003 [https://perma.cc/S24Q-Z2LQ].

149. William Turton & Kartikay Mehrotra, *Hacker Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 3:58 PM), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/25D5-R3LG].

and therefore are less likely to defend the attack in a timely manner.[150] Although in 2013 half of U.S. adults had personal information stolen due to hacking, less than half of American companies implement security measures to protect consumer information.[151]

F. Ransomware in the Setting of HIT

Ransomware in the healthcare context has become an exponentially increasing focus due to the high-stakes nature of healthcare, personal information stored, and potential for large payouts.[152] The ransomware industry in the medical realm has skyrocketed in the last decade, with some studies reporting increases of 350%.[153] Health facilities are a naturally vulnerable and rich target for hacking since they store the most intimate personal health and financial information, ideal for profit on the black market.[154] They are a uniquely ideal victim due to their need to return to functionality and usually acquiesce the hacker's request quickly in order to provide critical care to patients that would be near impossible without EHR access.[155] Initially, PHI exfiltration began with the basic physical stealing of laptops from within healthcare institutions.[156] This quickly has progressed to large-scale assaults unencumbered by wires or physical hardware.[157] As previously mentioned, the network, EHR, and internet are distinct, yet so interwoven that their demarcating lines are becoming increasingly blurred.[158] An attack does not commence directly

150. Hannah Mitchell, *FBI, CISA Warns Ransomware Attacks Surge Over Holiday Weekends: 6 Things to Know This Labor Day Weekend*, BECKER'S REV.: HEALTH IT (Sept. 1, 2021), https://www.beckershospitalreview.com/cybersecurity/fbi-cisa-warns-ransomware-attacks-surge-over-holiday-weekends-6-things-to-know-this-labor-day-weekend.html [https://perma.cc/R4BZ-GFRN]; *see also* E-mail from Beth Nielsen, Security Manager, Crystal Run Health, to Tien Lau, Physician, Crystal Run Health (Sept. 3, 2021, 1:21 PM) (on file with author) [hereinafter Nielsen E-mail].

151. LISA G. LERMAN & PHILIP G. SCHRAG, ETHICAL PROBLEMS IN THE PRACTICE OF LAW 152-53 (Erwin Chemerinsky et al. eds., 4th ed. 2016).

152. LastWeekTonight, *supra* note 13; Janardhanan, *supra* note 25, at 668.

153. Thomas J. Shaw, *Ransomware – The Legal Impacts*, 32 HEALTH L., Aug. 2020, at 32.

154. Farringer, *supra* note 16, at 952; Mariya Yao, *Your Electronic Medical Records Could Be Worth $1000 to Hackers*, FORBES (Apr. 14, 2017, 10:05 PM), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/?sh=4c3373c650cf [https://perma.cc/X5KB-Y9VM].

155. Nikki Spence et al., *Ransomware in Healthcare Facilities: A Harbinger of the Future?*, PERSPS. IN HEALTH INFO. MGMT. (June 29, 2018), https://web.archive.org/web/20211025015101/https://perspectives.ahima.org/ransomwareinhealthcarefacilities [https://perma.cc/8PFZ-E94M].

156. Cindy Gallee, *The Importance of Data Encryption and Security Rules: Breaches of Electronic Protected Health Information Under HIPAA and HITECH*, 26 DCBA BRIEF, June 2014, at 16, 20, https://www.dcba.org/mpage/vol260614art1 [https://perma.cc/AC2E-L5MP].

157. Farringer, *supra* note 16, at 951.

158. Ahrens E-mail, *supra* note 90.

upon the EHR, but more commonly indirectly within the network, originating either from the internet as in phishing, or locally uploaded onto the network via a device, such as a USB drive.[159] The virus attempts to find a weak link in the network chain in the form of a poorly secured device.[160] Once populated onto this primary device, the virus replicates in a "lateral movement" attack, spreading to other machines to which the primary device is connected via the intranet.[161] For example, an X-Ray machine, through HIT and connected to the network, usually possesses little security software and would be easy for a virus to infiltrate and then spread laterally.[162] Similarly, a patient's pacemaker or other personal device with wireless communication functionality may be hacked to the detriment of the patient directly or the healthcare institution via lateral movement.[163] In this fashion, the hacker may indirectly access and lock a key server, rendering the entire network unusable.[164]

Ransomware targeting HIT affects healthcare institutions in two distinct ways.[165] The first and perhaps most obvious danger is the exfiltration of PHI, which the hacker may hold ransom until a sum is paid, threatening to sell or distribute the sensitive information.[166] Essentially, this type of hack affects past patients, whose data was already stored within the hospital's digital records at a previous time.[167] In addition to PHI, other stored information within the EHR include financial identifications, the exposure of which could lead to identity theft.[168] The security of PHI is taken extremely seriously at baseline by healthcare institutions, which implement standardized training to all staff upon initial hiring with annual refreshers and corporate compliance modules to ensure HIPAA compliance.[169] Violation of these security

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*

163. Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart [https://perma.cc/ZW5T-Y9V4] (explaining that former Vice President Dick Cheney's physician disabled his pacemaker's wireless option for fear of potential assassination attempts by hackers).

164. Spence et al., *supra* note 155.

165. Farringer, *supra* note 16, at 952.

166. Janardhanan, *supra* note 25, at 668.

167. Farringer, *supra* note 16, at 952.

168. Janardhanan, *supra* note 25, at 668-69.

169. E-mail from Greg Radinsky, Chief Corp. Compliance Off., Northwell Health, to Elizabeth Stachtiaris, Physician, Northwell Health (Sept. 9, 2021, 7:20 PM) (on file with author [hereinafter Radinsky E-mail] (detailing that an employee who inappropriately accessed confidential patient

measures can lead to termination and potential civil or criminal penalties.[170] When a data breach occurs and affects personal information of 500 or more individuals, the institution is required to report the occurrence to the Secretary of Health and Human Services immediately and notify the affected persons within sixty days of discovery of the infiltration.[171] Such large-scale data breaches have been the focus of several class action lawsuits against corporate health systems, such as in *Fero v. Excellus Plan, Inc*.[172] In this case, the defendant health system was alleged to be negligent for not addressing lapses in security for more than nine months, during which hackers had unfettered access to approximately ten million individuals' PHI that had the potential for misuse.[173] Cases, such as *Fero*, which shed light on the insecurities of data storage in medical facilities[174] may discourage individuals from seeking medical care due to embarrassment if PHI were exfiltrated and published publicly or sold, leading to identity theft.[175]

While data breaches and attacks on PHI remain a growing problem for identity theft of prior patients,[176] ransomware targeting the denial of provider entry into the network and EHR system is exponentially rising and arguably more emergent as it affects present and future patient encounters in real time.[177] Blocking clinician access to the EHR until the healthcare corporation pays a ransom fee has devastating effects on the workflow of active patient care.[178] Most apparently, the inaccessibility of the EHR forces clinicians to use a backup system, usually comprising paper charts and order sheets.[179] In addition to being cumbersome, impromptu paper records are more susceptible to human error and more likely to be lost, thus further delaying patient care.[180] Lab and imaging results are also delayed, further decelerating the throughput of patient

---

records was terminated from the institution and the respective patients were informed of the PHI breach).

170. *Id.*

171. The Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 17932; *see also* U.S. Dep't of Health and Human Servs., *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, OFF. C.R., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [https://perma.cc/288F-XWFA] (last visited Aug. 12, 2023).

172. 502 F. Supp. 3d 724, 731 (W.D.N.Y. 2020).

173. *Id.*

174. *Id.*

175. Janardhanan, *supra* note 25, at 669.

176. *Id.* at 668.

177. Spence et al., *supra* note 155.

178. Fieldings E-mail, *supra* note 5.

179. Farringer, *supra* note 16, at 939; *see also* Dowlat, *supra* note 84.

180. Fieldings E-mail, *supra* note 5.

care.[181] Moreover, the inability to access the prior health record of a patient blinds physicians to crucial information, such as previously recorded medical history and allergies, which may not be communicable by a patient lacking capacity or *in extremis*.[182] While emergency rooms cannot reject patients without at least a medical screening exam and resuscitation care as per EMTALA,[183] pre-arranged appointments were cancelled, ambulances were diverted to other nearby emergency rooms from dispatch, and patients were transferred to other hospitals once stabilized.[184] The ransomware attack on the MedStar health system in 2016 devastated all ten of its hospitals in the Maryland and Washington, D.C. area[185] until the demand for forty-five Bitcoin, which is the equivalent of $19,000, was paid in exchange for the keycode to deactivate the virus and restore the HIT programs.[186] To a multibillion dollar corporation,[187] this price seems miniscule compared to the damage caused by the ransomware, and paying the fee resolves the issue more quickly than investigation by the FBI, which advises hospitals to avoid paying ransoms for fear that the problem will multiply to other healthcare facilities.[188] Even if hospitals refuse to pay the ransom, hospitals still may lose tens of millions of dollars in revenue and fixing the issue.[189] In addition to the backup system of paper charting, some hospitals have incorporated a "read-only" function within their EHR to allow the clinician access to the patient's prior records containing vital

181. I. Glenn Cohen et al., *Your Money or Your Patient's Life? Ransomware and Electronic Health Records*, PETRIE-FLOM CTR. FOR HEALTH L. POL'Y, BIOTECHNOLOGY AND BIOETHICS AT HARV. L. SCH. (Sept. 19, 2017), https://petrieflom.law.harvard.edu/resources/article/your-money-or-your-patients-life-ransomware-and-electronic-health-records [https://perma.cc/G7XM-Q42J].

182. *Id.*; *see also* Fieldings E-mail, *supra* note 5.

183. The Emergency Medical Treatment and Labor Act, 42 U.S.C § 1395dd(a)–(b) (2000).

184. Pete Williams, *MedStar Hospitals Recovering After "Ransomware" Hack*, NBC NEWS (Mar. 31, 2016, 2:53 PM), https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121 [https://perma.cc/BE6J-KZDF]; Cox, *supra* note 9.

185. Williams, *supra* note 184.

186. Jack McCarthy, *MedStar Attack Found to Be Ransomware, Hackers Demand Bitcoin*, HEALTHCARE IT NEWS (Apr. 4, 2016, 9:26 AM), https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin [https://perma.cc/HFM2-HKME].

187. *Facts and Figures*, MEDSTAR HEALTH, https://www.medstarhealth.org/mhs/about-medstar/facts-and-figures [https://perma.cc/2JCL-WXSS] (last visited Aug. 12, 2023).

188. Rachel King, *FBI Cyber Division Chief Advises Companies Not to Pay Ransom for Release of Data*, WALL ST. J. (May 4, 2016, 1:24 PM), https://www.wsj.com/articles/BL-CIOB-9679 [https://perma.cc/EM24-23R3].

189. *See* Stacy Weiner, *The Growing Threat of Ransomware Attacks on Hospitals*, AAMC (July 20, 2021), https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals [https://perma.cc/W7AV-2U43] (detailing how the ransomware attack on University of Vermont Medical Center cost $50 million in both lost revenue and continuous IT workers battling the network virus while incorporating a paper chart backup system).

information;[190] however, this workaround does not negate the increased propensity of human error without technomedicine, delays in care, and gridlock of patient throughput.[191]

G. HIPAA

Medicine and law, though distinct vocations, have become increasingly intertwined, especially within the last few decades.[192] HIPAA, one of the many laws overseeing the practice of medicine, governs the privacy of patient PHI across multiple media by mutual providers and third-party payers.[193] Enacted in 1996, it sought two goals: to provide for the maintenance of health insurance after employment termination[194] and to protect PHI and confidentiality as medical facilities embraced HIT.[195] It was reinvigorated in 2003 with the separate Privacy Rule and Security Rule with the aspiration that by 2004, nearly all medical records would be fully transitioned to electronic for the purpose of sharing information securely between providers with the patient's authorization.[196] Physicians constantly bear HIPAA on their shoulders with every patient encounter, ensuring discretion with PHI and obtaining consent prior to verbal or written disclosure to family members or employers.[197] While patient consent for disclosure amongst covered entities, such as other mutual clinicians or hospitals, is optional under the Privacy Rule,[198] many states have adopted policies and laws

190. E-mail from LaRay Brown, Chief Exec. Off., One Brooklyn Health, to Elizabeth Stachtiaris, Physician, Brookdale Hospital Medical Ctr. (Dec. 2, 2022, 2:53 PM) (on file with author) [hereinafter Brown E-mail].

191. Fieldings E-mail, *supra* note 5.

192. Joyce Frieden, *Mixing Medicine and Law*, MEDPAGE TODAY (Jan. 7, 2015), https://www.medpagetoday.com/opinion/inotherwords/49407 [https://perma.cc/8BNQ-3QGJ].

193. The Health Information Portability and Accountability Act of 1996, Pub. Law No. 104-191, § 1177, 110 Stat. 1936, 2029.

194. *Continuation of Health Coverage (COBRA)*, U.S. DEP'T OF LABOR, https://www.dol.gov/general/topic/health-plans/cobra [https://perma.cc/LG5C-DJJM] (last visited Aug. 12, 2023).

195. Farringer, *supra* note 16, at 942.

196. *Id.*; *see also Fact Sheet: Transforming Health Care for All Americans*, WHITE HOUSE PRESS SEC'Y (May 27, 2004), https://georgewbush-whitehouse.archives.gov/news/releases/2004/05/20040527-2.html [https://perma.cc/UZ4A-CV22].

197. *Sharing Health Information with Family and Friends*, U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. C.R., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf [https://perma.cc/AZV3-XEZH] (last visited Aug. 12, 2023) [hereinafter *Sharing Health Information*] (omitting the requirement of overt consent and allowing information sharing in the absence of objection).

198. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/J6NV-35KK] (last visited Aug. 12, 2023).

requiring it.[199] Although most EHRs across hospital systems do not communicate, those that do interact contain forms that, once printed and signed by the patient, allow the provider access to the EHR of a prior visit at another hospital, thereby giving the clinician sophisticated medical history that the patient may not be able to provide verbally.[200]

H. HITECH

The HITECH Act is one of several subdivisions of the American Recovery and Reinvestment Act ("ARRA") of 2009,[201] which aspired to boost the economy and allot more budget to healthcare after the 2008 depression.[202] HITECH builds upon HIPAA by altering the Privacy Rule and certain other aspects with a more patient-centric focus—for example, prohibiting marketing to patients via the EHR as was previously permitted under HIPAA unless medically necessary for the patient's specific condition.[203] Moreover, personal access to the patient's own PHI was made easier to obtain electronically.[204] While HIPAA's goal was to convert all health records to EHR, it lacked enforcement, resulting in a trickling transition,[205] whereas HITECH financially incentivized providers to adopt EHR and comply with its "meaningful use standards," but penalized those facilities which did not conform within four years.[206] HITECH jettisoned commercial medical practice into the world of reliance on technomedicine, perhaps before it was actually ready with proper safeguards in place, while leaving smaller clinics and private practices to either perish or suffer the significant financial burden of EHR.[207] HITECH essentially mandated all medical practitioners, regardless of financial ability, to adopt and utilize EHR and subsequently left them vulnerable to ransomware without sufficient

199. *Patient Consent for Electronic Health Information Exchange and Interoperability*, HEALTHIT.GOV, https://www.healthit.gov/topic/interoperability/patient-consent-electronic-health-information-exchange-and-interoperability [https://perma.cc/WZ86-5ZEY] (last visited Aug. 12, 2023).

200. *Privacy, Security, and Electronic Health Records*, OFF. C.R., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf [https://perma.cc/5UTU-RZ6U] (last visited Aug. 12, 2023).

201. American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001, 123 Stat. 115, 226.

202. Janardhanan, *supra* note 25, at 669.

203. Lisa L. Dahm, *Carrots and Sticks in the HITECH Act: Should Covered Entities Panic?*, 22 HEALTH L. 1, 6 (2010).

204. Howard Burde, *The HITECH Act—An Overview*, 13 AM. MED. ASSOC. J. ETHICS 172, 174 (2011).

205. Farringer, *supra* note 16, at 945.

206. *Id.* at 945-46.

207. *Id.* at 946.

safeguards, forcing them to potentially take on even more expenses for security.[208]

While demanding the abrupt transition to EHR, the HITECH Act itself omits specific security measures; rather, it defers such regulations to the Office of the National Coordinator for Health Information Technology ("ONCHIT").[209] ONCHIT was created to oversee the nationwide implementation of HIT across both the public and private sectors of healthcare.[210] In turn, ONCHIT issued several contracts to other subcommittees, such as the American National Standards Institute ("ANSI") and the Certification Commission for Healthcare Information Technology ("CCHIT") to formulate and adopt standards by which HIT must be certified, as well as the Health Information Security and Privacy Collaboration ("HISPC") to incorporate HIPAA provisions.[211] This maze of contracts and deferred responsibilities results in specific safety regulations omitted from the HITECH Act, forcing individual healthcare entities to finagle their own compliance with HIPAA and HITECH, resulting in security variations across institutions.[212] Further, while HITECH names "network" in the setting of "nationwide health information network," it does not define it in the context of a local institution's HIT system nor contrast it from the internet.[213]

I. EMTALA

EMTALA was enacted in 1986 to ensure that those individuals presenting to an emergency department for any life or limb threatening pathology would receive proper care, regardless of their financial status or insurance carrier.[214] It was nicknamed the "Patient Anti-Dumping Law" in the wake of some hospitals, which received federal funding, refusing to treat patients for whom payment was not certain.[215] At the most extreme end of the spectrum, this would lead to patients dying en

208. Ahrens E-mail, *supra* note 90.

209. The Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001, 123 Stat. 115, 230.

210. C. STEPHEN REDHEAD, CONG. RSCH. SERV., R40161, THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT 7, 8 (2009).

211. *Id.* at 7.

212. Ahrens E-mail, *supra* note 90.

213. HITECH Act §§ 3001–02.

214. *Emergency Medical Treatment & Labor Act*, CTRS. FOR MEDICARE & MEDICAID SERVS. (Dec. 2, 2021, 8:00 PM), https://www.cms.gov/Regulations-and-Guidance/Legislation/EMTALA [https://perma.cc/D5CT-KA2R].

215. *1986—Ending Hospital "Dumping,"* NAT'L HEALTH L. PROGRAM, https://healthlaw.org/announcement/ending-hospital-dumping-1986 [https://perma.cc/E9ZC-2S2X] (last visited Aug. 12, 2023).

route while attempting to find a hospital that would treat them.[216] The statute also extends not only to pure medical treatment, but to obstetric resuscitation.[217] If a patient presents to the emergency department with an ailment requiring a specialty which that hospital does not offer, treating staff must first stabilize[218] the patient prior to transferring to a different healthcare facility for a high level of care.[219] If the initial facility has the ability to provide the needed service, a hospital-initiated transfer based on patient preference and not on necessity, thus not invoking EMTALA's emergency medical condition provision for "appropriate transfer," is disallowed and must be undertaken by the patient or their family at their own expense.[220]

III. LEGAL ISSUE

The legal dilemmas that arise throughout the practice of medicine are myriad, yet are nevertheless raised exponentially when HIT is incorporated, especially to the reliance of both clinicians and patients.[221] Part III of this Note delves into these issues and precedes their respective proposed solutions.[222] Part III.A describes the gravest consequence of ransomware targeting HIT: blocked entry into the EHR preventing physicians from delivering real-time care to instant patients, leading to devastating outcomes for both the healthcare institution and the patients themselves.[223] Next, Part III.B delineates the more notorious

---

216. *See* David A. Hyman, *Patient Dumping and EMTALA: Past/Imperfect and Future Shock*, 8 HEALTH MATRIX: J.L.-MED., 29, 34-35 (1998) (presenting a notorious anecdote of Mr. Takewell, who suffered from chronic poorly controlled diabetes and presented to a hospital in a diabetic coma after already incurring a large medical debt there due to being uninsured and unemployed). The vignette further explains that a hospital administrator physically lifted him from the emergency room and left him on the ground of an adjacent parking lot, and he subsequently died the next day. *Id.* at 35.

217. *Jury Awards Woman $200,000 After Hospital ED Sends Her Home to Deliver Her Dead 16-Week-Old Fetus*, RELIAS MEDIA (July 1, 2011), https://www.reliasmedia.com/articles/131042-jury-awards-woman-200-000-after-hospital-ed-sends-her-home-to-deliver-her-dead-16-week-old-fetus [https://perma.cc/92YN-FL84] (chronicling *Morin v. Eastern Maine Medical Center*). In *Morin*, the plaintiff had been discharged from the emergency room after being diagnosed with intrauterine fetal demise and subsequently delivered the dead fetus in her bathtub, later prevailing in her claim that her emergency medical condition was not stabilized prior to discharge in violation of EMTALA. Morin v. E. Me. Med. Ctr., 780 F. Supp. 2d 84, 91-92 (D. Me. 2010).

218. Hyman, *supra* note 216, at 31.

219. EMTALA, 42 U.S.C § 1395dd(c)(1) (2000).

220. *Emergency Medical Treatment and Active Labor Act*, ILL. HEALTH & HOSP. ASSOC., https://www.team-iha.org/files/non-gated/legal/emtala-summary.aspx [https://perma.cc/2G4B-GGB5] (last visited Aug. 12, 2023).

221. *See generally infra* Part III.

222. *See infra* Part III–IV.

223. *See infra* Part III.A.

repercussion of EHR ransomware that has been publicized throughout the media, namely the exfiltration of PHI with threats of its mass distribution should the institution fail to pay the demanded cryptocurrency, thus violating the Privacy and Security Rules of HIPAA.[224] Part III.C exposes the crux of the security issue: that since the local network is essentially ignored in legislation, it is also neglected within healthcare facilities, yet it is the secret key target of hackers to infiltrate a hospital's HIT.[225] Part III.D builds upon Part II.H, which highlights the lack of uniformity among healthcare institutions regarding HIT security regulations, leading to some facilities being more vulnerable than others to ransomware attacks.[226]

A. Ransomware and Blocked Entry

Once ransomware has overtaken a hospital, an emergent dilemma manifests that hinders the care of present and future patients: denial of service to the EHR, upon which physicians rely to deliver efficient and sound care in real time.[227] The unavailability of patient records denies the clinicians crucial information, such as past medical history, prior treatments, and allergies.[228] As detailed above, this can lead to catastrophic effects suffered by patients, including duplicate therapies, medication errors, and deaths.[229] Most patients cared for within a hacked institution are unaware of the infiltration at the beginning of their visit.[230] In addition, this leads to difficulties suffered by the hospital, including increased length-of-stays, lost revenue, and increased staffing requirements to conquer the virus.[231]

---

224. *See infra* Part III.B.

225. *See infra* Part III.C.

226. *See infra* Part III.D.

227. *See* Farringer, *supra* note 16, at 940.

228. Paul Frysh, *How Hackers Hold Hospitals, and Your Health, for Ransom*, WEBMD (Mar. 30, 2021), https://www.webmd.com/a-to-z-guides/story/how-hackers-hold-hospitals-for-ransom [https://perma.cc/36YQ-ZXK9].

229. Mike Miliard, *Hospital Ransomware Attack Led to Infant's Death, Lawsuit Alleges*, HEALTHCARE IT NEWS (Oct. 1, 2021, 1:31 PM), https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges [https://perma.cc/2TSJ-AUJ7] (telling an anecdote of ransomware allegedly contributing to an infant's avoidable death). Had ransomware not rendered HIT inoperable in the hospital, fetal heart monitors could have warned physicians of fetal distress early and prompted a preemptive C-section, thus preventing the subsequent brain injury caused by a nuchal cord. *See id.*

230. *See, e.g.*, *id.* (explaining further that the pregnant patient was not informed of the cyberattack when she arrived for her scheduled labor induction; however, since this visit was expected and therefore nonemergent, the institution could have informed her and she could have chosen to attend a different site with functional HIT, potentially avoiding the poor outcome).

231. Danny Palmer, *Ransomware Attacks Against Hospitals Are Having Some Very Grim Consequences*, ZDNET (Sept. 29, 2021), https://www.zdnet.com/article/ransomware-attacks-

EMTALA requires that anyone coming to an emergency department receive at least a medical screening exam, treatment, and stabilization, regardless of their ability to pay.[232] When cyberattacks bring the emergency room to a screeching halt by slowing down the workflow of physicians and taking away the essential EHR,[233] patients build up in the waiting room.[234] This leads to patients waiting several hours before initial evaluation, leading to worsening of the patient's condition or even death.[235] Even if patients are timely screened, hindering EHR access can deny providers vital information, such as details of prior visits that the patient cannot remember or if the patient is nonverbal or *in extremis*.[236] Present information is already lost in communication without the EHR, including the most basic material of a medical encounter, such as vital signs.[237] This will preclude physicians from providing proper specialized treatment required for each individual.[238] Therefore, ransomware blocking entry into HIT arguably forces the healthcare institution and its clinicians to violate EMTALA.[239]

B. PHI Exfiltration

Additionally, after a ransomware attack has ensued, past patients are at risk of their PHI being exfiltrated and exposed.[240] While ARRA and HITECH aimed to modernize the medical industry, they introduced their demands prematurely, forcing healthcare facilities of all specialties

---

against-hospitals-are-having-some-very-grim-consequences [https://perma.cc/XHM8-9R7A]; *see also* Weiner, *supra* note 189.

232. *Understanding EMTALA*, AM. COLL. OF EMERGENCY PHYSICIANS, https://www.acep.org/life-as-a-physician/ethics--legal/emtala/emtala-fact-sheet [https://perma.cc/TT46-W8HW] (last visited Aug. 12, 2023).

233. Palmer, *supra* note 231.

234. Chadd K. Kraus, *The Emergency Department Waiting Room: A Barometer of Hospital Throughput and Capacity?*, 1 J. AM. COLL. EMERGENCY PHYSICIANS OPEN 1060, 1060 (2020).

235. Michael Rubinkam, *Suit: 'Abandoned' Man Dies in Hospital Waiting Room*, AP NEWS (Aug. 5, 2021), https://www.usnews.com/news/best-states/pennsylvania/articles/2021-08-05/suit-abandoned-man-dies-in-hospital-waiting-room [https://perma.cc/B662-LGF8] (exposing that a man, the subject of a wrongful death suit, died while waiting over two hours to be initially assessed in an emergency department waiting room, allegedly due to understaffing, which was a known, yet uncorrected, issue).

236. Fieldings E-mail, *supra* note 5.

237. *Id.*

238. *See Improved Diagnostics & Patient Outcomes*, HEALTH IT, https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/improved-diagnostics-patient-outcomes [https://perma.cc/389H-TW6Y] (last visited Aug. 12, 2023) (explaining that when healthcare providers have access to complete and accurate information, namely via EHR, they are able to provide better care to patients).

239. *See id.* (implying that the lack of EHR produces worse patient satisfaction and outcomes); *see also* Rubinkam, *supra* note 235.

240. Janardhanan, *supra* note 25, at 668.

and size to adopt EHR, regardless of financial ability to independently secure it or organizational readiness.[241] However, HITECH does not specify precise security measures that would maintain HIPAA compliance, but rather defers this to ONCHIT, which in turn defers to several subcommittees.[242] This inevitably leads to variations in HIT safeguards across individual institutions, leaving some more vulnerable than others, especially those in underserved communities with limited funding.[243]

While EHR companies are not required to be compliant with HIPAA, healthcare institutions are, placing the burden on said facilities.[244] Furthermore, a hospital would not utilize an EHR system that hindered HIPAA compliance, therefore incentivizing EHR systems to allow such amenability.[245] However, there are drastic differences between EHR systems, especially in the areas of user-friendliness accessibility.[246] PHI is more vulnerable to hacking than most other stores of information because of its fluidity due to a patient's ever-evolving clinical course and the need for a patient's ability to access their own chart.[247] It also contains most intimate information, including medical history and private billing identifiers, such as one's social security number.[248] Additionally, certain EHR systems and certain healthcare facilities are more prone to hacking, such as private practices and clinics which utilize EHR systems accessible via an internet browser.[249]

The lack of uniformity in EHR safeguards, resulting in hacking and ransomware targeting HIT and exfiltrating PHI, places the hospital at risk for breaching HIPAA.[250] Further, the mandate to adopt EHR from

241. Farringer, *supra* note 16, at 946.

242. REDHEAD, *supra* note 210, at 8.

243. Ahrens E-mail, *supra* note 90.

244. *Id.*

245. *Id.*

246. PRAXIS, *supra* note 118.

247. Ross Koppel & Craig Kuziemsky, *Healthcare Data Are Remarkably Vulnerable to Hacking: Connected Healthcare Delivery Increases the Risks*, 257 STUD. HEALTH TECH. INFO. 218, 218-19 (2019); *see also* Nicole Wetsman, *Third-Party Health Apps Are Vulnerable to Hacks, Report Finds*, VERGE (Oct. 18, 2021, 12:32 PM), https://www.theverge.com/2021/10/18/22732615/health-record-app-hacks-patinet-data [https://perma.cc/5QSS-Z28Q] (explaining that once secured PHI exits the EHR, it is less protected from outside threats, including personal phone applications requesting health information synced from an official EHR chart, even if requested by the patient himself).

248. Yao, *supra* note 154; *see also* Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SECURELINK (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers [https://perma.cc/TJY8-8NXT].

249. Ahrens E-mail, *supra* note 90.

250. *Id.*

HITECH exposed institutions to increased HIPAA liability.[251] When hackers retrieve PHI, it is considered a disclosure, which is forbidden under the HIPAA Privacy Rule.[252] Data breaches affecting 500 or more individuals require the institution to report the occurrence under HIPAA to the Secretary of Health and Human Services immediately and notify the affected persons within sixty days of discovery of the infiltration.[253]

PHI exfiltration is the more commonly reported form of ransomware when a hacker extorts PHI for payment under the threat of its publication, usually on the internet.[254] While this is not as serious as ransomware blocking entry into the EHR system, thus hindering care to present patients in real time,[255] it affects more people at one instance insofar as it risks the personal PHI of potentially all past patients of an institution rather than the ones residing within the institution in the present.[256] This risk of ransomware exfiltrating PHI places the facility liable under HIPAA for the potential eternity even after the patient is discharged, unless foolproof safety measures are implemented.[257] The institution is more so liable if it is aware of security flaws, yet fails to correct them for a substantial period of time, leading to a PHI breach.[258]

C. Neglecting the "Network"

While both HITECH and HIPAA emphasize EHR, they ironically do not mention the basic local network upon which it operates, which is in fact the key target in the commencement of an attack via lateral movement.[259] HITECH names "network" in the setting of "nationwide health information network," but it does not define it in the context of a

251. Farringer, *supra* note 16, at 941.

252. *Healthcare for Ransom: A Look into the HIPAA Guidelines for Ransomware Incidents*, TREND MICRO (Sept. 7, 2016), https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/healthcare-for-ransom-a-look-into-the-hipaa-guidelines-for-ransomware-incidents [https://perma.cc/B5VG-SSZF].

253. The Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402, 123 Stat. 226, 261 (codified as amended 42 U.S.C. § 13001–14002); *see also* U.S. Dep't of Health and Human Servs., *supra* note 171.

254. Farringer, *supra* note 16, at 952.

255. *See supra* Part III.A.

256. Fero v. Excellus Health Plan, Inc., 502 F. Supp. 3d 724, 733-34 (W.D.N.Y. 2020) (demonstrating that during a PHI breach, hackers had access to over ten million individuals' PHI).

257. *PHI of 1.27 Million Patients Compromised in Two Healthcare Data Breaches*, HIPAA J. (Nov. 16, 2021), https://www.hipaajournal.com/phi-of-1-27-million-patients-compromised-in-two-healthcare-data-breaches [https://perma.cc/JDR9-66DE].

258. *See* Jacqueline LaPointe, *MedStar Ransomware Attack Caused by Known Security Flaw*, HEALTH IT SEC. (Apr. 7, 2016), https://healthitsecurity.com/news/medstar-ransomware-attack-caused-by-known-security-flaw [https://perma.cc/9WE4-8XEE].

259. Ahrens E-mail, *supra* note 90.

local institution's HIT system nor contrast it from the internet.[260] As previously mentioned, this distinction between the local network and the internet is crucial to understanding the machinations of ransomware targeting HIT.[261] Most HIT viruses begin on the network as a link sent via an e-mail on the internet and then spread laterally and propagate to the EHR, leading to devastating outcomes.[262] Rarely do hackers directly target the EHR.[263] Therefore, defending the network is key to preventing ransomware attacks and decreasing the vulnerability of healthcare institutions.[264] The HITECH Act starkly ignores mention of the local network,[265] yet forces healthcare facilities, no matter the size or financial ability, to adopt HIT and EHR at the peril of violating HIPAA without a scintilla of ensured safety.[266] While technology has vastly transformed and rapidly advanced in this last century,[267] there have been no updates or amendments made to the security regulations issued under HIPAA since its finalization in 2003.[268] They are henceforth out of date and do little to protect institutions against cyberattacks.[269] Under threat of penalty, the HITECH Act leaves the institution defenseless against ransomware and alone to suffer the legal consequences of disclosure against HIPAA.[270]

D. Differences Across Institutions

The legislature's failure to address the local network as the most fundamental aspect of ransomware creates a loophole for hackers to enter and spread laterally, eventually finding the indirect target within

260. The Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13101, 123 Stat. 226, 230-34.

261. *See supra* Part II.D.

262. Ahrens E-mail, *supra* note 90.

263. *Id.*

264. *Id.*

265. HITECH Act §§ 3001–02.

266. Ahrens E-mail, *supra* note 90.

267. *See generally 100 Years of Advancement – How Has Technology Developed from 1920-2020?*, ENSIGN (Dec. 27, 2019), https://www.ensign-net.co.uk/100_Years_of_Advancement-How_has_Technology_Developed_from_1920-2020.html [https://perma.cc/Y5KB-T2WL?type=image].

268. Farringer, *supra* note 16, at 948.

269. Elizabeth Snell, *Is the HIPAA Security Rule Doing Enough for Healthcare?*, HEALTHITSECURITY (Apr. 22, 2015), https://healthitsecurity.com/news/is-the-hipaa-security-rule-doing-enough-for-healthcare [https://perma.cc/D5K4-TQU7].

270. Ahrens E-mail, *supra* note 90.

the EHR.[271] The dearth of uniform safety regulations, or at least minimum-security measures, leads healthcare institutions to have differing safeguards against cyberattacks.[272] While the advanced intricacies of modern malware admittedly demand some variation between facilities so as to not make each target identical, some facilities are left essentially defenseless to cyberattacks, especially those with less profits such as community hospitals or private practices.[273]

Presently, healthcare facilities incorporate inconsistent safety measures, leaving their institutions at differing levels of vulnerability to hackers.[274] For example, certain institutions block some websites notoriously ridden with virus entry points like social media pages and personal e-mail accounts, while others do not.[275] While HIT encompasses not only the EHR—but also the network, intranet, third-party programs such as PACS, and other hardware such as X-Ray machines—one's username and password are usually the same, which increases the likelihood of infiltration if login information is learned from one source.[276] Other protections include the prohibition of personal external storage devices, such as USB drives, which can propagate compromised material onto the network either with or without the owner's knowledge.[277] These security measures should be present more uniformly across all healthcare facilities so that one institution may not become more vulnerable than another.[278]

---

271. Katey Wood, *Ransomware Reduction 101: Lateral Movement Between Endpoints*, ILLUMIO (Dec. 14, 2020), https://www.illumio.com/blog/endpoint-lateral-movement [https://perma.cc/S27Z-X9K8].

272. Ahrens E-mail, *supra* note 90.

273. *Id.*

274. *Id.*

275. Northwell Health Policy Committee, *Acceptable Computer Use Policy*, NORTHWELL HEALTH (Mar. 7, 2022) (on file with Northwell Health) [hereinafter *Northwell Acceptable Computer Use Policy*] (describing specific allowable and barred practices that employees may perform on HIT within the health system, including the preclusion of access to websites with objectionable content).

276. Northwell Health Policy Committee, *Password Policy*, NORTHWELL HEALTH (Aug. 10, 2021) (on file with Northwell Health) [hereinafter *Northwell Password Policy*] (describing the health system's protocol for password requirements, including the strength of the password itself via the utilization of certain characters, multi-factor authentication, and frequent password changes); *see also* E-mail from the Northwell Information Services, Northwell Health, to Elizabeth Stachtiaris, Physician, Northwell Health (Dec. 23, 2021, 6:45 AM) (on file with author) [hereinafter Northwell Information Services E-mail] (reminding all employees with EHR and network access to periodically change their passwords).

277. *Northwell Acceptable Computer Use Policy*, *supra* note 275; *see also Security Tip (ST08-001) Using Caution with USB Drives*, CISA (Apr. 28, 2011), https://www.cisa.gov/uscert/ncas/tips/ST08-001 [https://perma.cc/5PJR-JFCN?type=image].

278. *See* Ahrens E-mail, *supra* note 90.

IV. PROPOSED LEGAL SOLUTION

Federal laws fall short of protecting healthcare institutions responsible for abiding by such regulations from outside threats and devastation by ransomware.[279] While some scholars believe that change should originate from within the individual institution and the healthcare industry itself,[280] this would lead to even more inconsistencies across facilities, leaving some more vulnerable to malware than others.[281] Part IV of this Note proposes recommendations to combat the aforementioned legal issues stated in Part III.[282] Part IV.A suggests amendments that should be made to the HITECH Act.[283] Part IV.B advocates for amendments to HIPAA to allow healthcare facilities to more successfully comply with its regulations and avoid inadvertent disclosure of PHI during a ransomware attack.[284]

A. Amendments to HITECH

The HITECH Act should undergo immediate revisions and amendments that focus on the local network as well as other common HIT since these are frequent entry points of hackers.[285] Rather than deferring security solely to ONCHIT,[286] HITECH should expressly specify minimum-security standards in order to avoid drastic variability across institutions, ultimately leading to more vulnerable hospitals and practices.[287] Specific emphasis must be aimed at protecting the network; this begins with amending HITECH to acknowledge the network as HIT's most basic forum rather than its omission.[288]

Minimum-security standards should include fundamentals, such as frequent password changes as well as the requirement of characters difficult to replicate and multi-factor identification, which may be done via a third-party application or other personal device.[289] All HIT, including personal devices on which PHI is accessed, must be secured

279. Ryan M. Krisby, *Health Care Held Ransom: Modifications to Data Breach Security & the Future of Health Care Privacy Protection*, 28 HEALTH MATRIX: J.L.-MED. 365, 383 (2018).
280. Farringer, *supra* note 16, at 983.
281. *See* Ahrens E-mail, *supra* note 90.
282. *See infra* Part IV.A–B.
283. *See infra* Part IV.A.
284. *See infra* Part IV.B.
285. Ahrens E-mail, *supra* note 90.
286. *See supra* Part II.H.
287. *See supra* Part III.D; Ahrens E-mail, *supra* note 90.
288. Ahrens E-mail, *supra* note 90.
289. *Northwell Password Policy*, *supra* note 276.

with anti-virus software.[290] All newly hired employees should be required to attend an interactive corporate compliance training focused on HIT security and must retake it annually.[291] Remote access to the EHR allowing the clinician to document in and access patient charts at home must be granted with only the most stringent guidelines and should only be set up in-house by the institution's IT department along with multi-factor identification.[292] HITECH should demand a more readily accessible and user-friendly backup system should the hospital fall victim to ransomware.[293] Additionally, all PHI and electronically stored data within a healthcare institution should be encrypted so that even if it is exfiltrated, it cannot be accessed or misused.[294] Of course, institutions such as larger hospitals or health systems may go above the minimum-security standards as they respectively see fit for their respective finances and risk assessment.[295]

As technology rapidly advances throughout society in the current age, further consideration should be lent to fingerprint or facial recognition to avoid inadvertent disclosures of protected information.[296] Currently, this secure technology exists for personal use devices, such as cellular phones.[297] In the healthcare setting, nurses obtain medication through the Pyxis system, which requires fingerprint access and medication accountability.[298] Since such technology is already ubiquitous both in medical and societal practice, the legislators should consider requiring such identity verification for HIT and PHI.[299]

---

290. Northwell Health Policy Committee, *Anti-Virus and Anti-Malware Policy*, NORTHWELL HEALTH (Mar. 3, 2023) (on file with Northwell Health) [hereinafter *Northwell Anti-Virus and Anti-Malware Policy*].

291. Northwell Health Policy Committee, *Information Technology Security Awareness and Training Policy*, NORTHWELL HEALTH (June 1, 2022) (on file with Northwell Health) [hereinafter *Northwell Information Technology Security Awareness and Training Policy*].

292. Northwell Health Policy Committee, *Remote Access Policy*, NORTHWELL HEALTH (Feb. 4, 2022) (on file with Northwell Health) [hereinafter *Northwell Remote Access Policy*].

293. *See* Krisby, *supra* note 279, at 384 (suggesting a "3-2-1 Rule" for data storage: "*three* copies of data, on *two* different types of media, with *one* of those copies being off site").

294. *Id.* at 385, 387.

295. Ahrens E-mail, *supra* note 90.

296. Heather Kelly, *Fingerprint and Face Scans Are the Future of Smartphones. These Holdouts Refuse to Use Them.*, WASH. POST (Nov. 15, 2019), https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them [https://perma.cc/63GP-RQQG].

297. *Id.*

298. Medical Shipment, *Pyxis MedStation ES System Overview- by Kelly Larrabee-Robke BD*, YOUTUBE (Apr. 24, 2020), https://www.youtube.com/watch?v=DHhBtujpMQ4 [https://perma.cc/V3GF-8LWT].

299. Erika Gimbel, *How Biometric Technologies Improve Healthcare Operations*, HEALTHTECH (Dec. 18, 2019), https://healthtechmagazine.net/article/2019/12/how-biometric-

B. Amendments to HIPAA

Since HITECH naturally flows as an extension of HIPAA, many of the proposed amendments to HIPAA will be redundant in the proposed amendments to HITECH.[300] Since medical practice is now impossible without technology and EHR, HIPAA must be updated to focus on electronic information, which was not a priority when it was originally enacted.[301] It "should require a minimum level of organizational cyber hygiene and resilience."[302] As previously alluded to,[303] HIPAA should explicitly require all HIT including the network to contain security protections and intrusion-prevention software.[304] "Break-the-glass" settings should be implemented more universally when accessing PHI.[305] Unauthorized breaches of PHI should be standardly met with adverse consequences by the offending employee as a zero tolerance policy.[306] Furthermore, except if the patient informedly opts out, when patient records are entered for any reason, even if accessed appropriately, a notification should be sent to the patient via their pre-selected method.[307]

V. CONCLUSION

Just as a virus rapidly devastates the state of health of an individual or, on a pandemic scale, large communities, so too can ransomware ravage not only one patient, but also an entire health system.[308] Ransomware, a virus of technology, not only affects actual health, but also the economics of individuals and institutions.[309] Technomedicine

---

technologies-improve-healthcare-operations [https://perma.cc/VQK3-3KAL]; Kelly, *supra* note 296.

300. *See supra* Part IV.A.

301. Farringer, *supra* note 16, at 948-49.

302. Krisby, *supra* note 279, at 388; *see also* Chris Brook, *What Is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More*, DIGITALGUARDIAN (Oct. 6, 2020), https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more [https://perma.cc/EKA7-XJ7R] (defining "cyber hygiene" as prudent steps taken by the individual and organization to protect its technology from compromise).

303. *See supra* Part IV.A.

304. Krisby, *supra* note 279, at 388.

305. Ahrens E-mail, *supra* note 90 (explaining "break-the-glass" as an extra step required to access PHI); *see also Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems*, YALE UNIV., https://hipaa.yale.edu/security/break-glass-procedure-granting-emergency-access-critical-ephi-systems [https://perma.cc/5U73-V23C] (last visited Aug. 12, 2023).

306. Radinsky E-mail, *supra* note 169.

307. E-mail from Great Neck OB/GYN Doctor Direct Support Staff, Great Neck OB/GYN, to Elizabeth Stachtiaris, Patient, Great Neck OB/GYN (Dec. 22, 2021, 9:07 PM) (on file with author) [hereinafter GNOB E-mail] (informing the patient of each time their chart is accessed, even if by the patient herself).

308. Fieldings E-mail, *supra* note 5.

309. LastWeekTonight, *supra* note 13.

has swiftly evolved over the last century with hackers following at an exponential rate, looking to infiltrate the neglected flaws in HIT and exploit a high-stakes vulnerable field.[310]

Legislation governing medical practice, specifically the HITECH Act and HIPAA, has failed to adapt to the technological changes in the medical field, thus leaving many institutions defenseless against such attacks.[311] As a result, ransomware targeting healthcare facilities has grown into a highly profitable market, grossing hundreds of millions of dollars, with the FBI predicting eventual sums of over one billion dollars.[312] Health systems usually pay the ransom against the advice of law enforcement as the payment is usually a cheaper and quicker solution than combatting the viral infiltration.[313] The hospitals are forced to deliver subpar care to patients as well as suffer economic blows without safeguards from the government.[314]

Ransomware disables HIT in the two common ways of blocked entry and PHI exfiltration.[315] The former is more acutely critical as it affects the active care of present patients currently seeking treatment within the hospital.[316] The latter has more widespread consequences as it involves past patients' PHI, which may amount to several million inadvertent disclosures under HIPAA.[317]

The HITECH Act threw the field of medicine into the technological revolution, forcing all healthcare institutions to adopt EHR regardless of financial ability, initially with incentives and ultimately with punishments.[318] Inherent in the HITECH Act is the necessity to prevent inadvertent disclosures forbidden by the outdated HIPAA.[319] Yet, neither Act provides any explicit provisions or safeguards against ransomware attacks, which have exponentially increased in the last few decades.[320] Moreover, both Acts overtly omit the mention of the local "network" on which an institution's HIT operates, despite it being the key target of most hackers for viruses to spread laterally and infect the EHR.[321]

310. Farringer, *supra* note 16, at 940-41.
311. *Id.* at 948.
312. Stackhouse, *supra* note 140.
313. King, *supra* note 188; Weiner, *supra* note 189; *see also* Ahrens E-mail, *supra* note 90.
314. *See supra* Part III.A.
315. *See supra* Part III.A–B.
316. *See supra* Part III.A.
317. *See supra* Part III.B.
318. Dahm, *supra* note 203, at 3, 6.
319. *See supra* Part II.H.
320. *See supra* Part III.
321. *See supra* Part III.

Both HITECH and HIPAA must themselves be jettisoned into the current era of technomedicine.[322] Amendments listing minimum-security measures are direly required in order to prevent drastic variability, which leads to disparities among vulnerable institutions.[323] Without public condemnation of HIT hacking, patients' lives and PHI remain at risk for the foreseeable future.[324]

*Elizabeth Stachtiaris, D.O.**

322. *See supra* Part IV.

323. *See supra* Part IV.

324. *See supra* Part III.

* J.D., 2023, *cum laude*, Maurice A. Deane School of Law at Hofstra University; D.O., 2016, New York College of Osteopathic Medicine; B.A., 2011, New York University. The publication of this Note would not be possible without the support and inspiration of several people, to whom I would like to express sincere gratitude. First, I would like to thank my mother, Lillian Stachtiaris, M.D., who always motivated me from a young age to aspire for greatness, never settle for mediocrity, and pursue a rewarding career of healing others. Next, I appreciate my husband, Tien Lau, D.O., who not only championed me through medical school and residency, but also law school, as well as the journey within *Hofstra Law Review*, namely the completion of the writing competition during our honeymoon and the production of this Note. Professor Janet Dolgin, J.D., the director of the Gitenstein Institute for Health Law and Policy at the Maurice A. Deane School of Law at Hofstra University, has encouraged my efforts in combining my two vocations of law and medicine in innovative ways I could not have imagined, including the composition of this Note. I would also like to acknowledge Ms. Adonza Anderson, who facilitated my attendance of law school after medical school and residency, allowing me to achieve my dreams of a legal education. Bill Ahrens patiently educated me, a tech-amateur, on the intricacies of HIT and ransomware. A great thanks to my physician colleagues, especially Tiffany Fieldings, M.D., who persevered through prolonged EHR downtime due to malware and continued to deliver excellent patient care, influencing this Note and preparing me for when I, myself, had the misfortune of experiencing medical ransomware firsthand. Finally, I would like to convey appreciation to the myriad patients and their loved ones, who allow us physicians to care for them during their vulnerable time of need. I would not be the physician, or person, I am today without any of the aforementioned individuals, and so many more.