Washington and Lee Journal of Civil Rights and Social Justice

Volume 25 | Issue 1 Article 9

3-11-2019

HealthTech: How Blockchain Can Simplify Healthcare Compliance

Kathryn M. Bennett
Washington and Lee University School of Law, bennett.k@law.wlu.edu

HealthTech[1]: How Blockchain Can Simplify Healthcare Compliance

Kathryn M. Bennett*

Abstract

This Note broadly explores solutions to modern-day accessibility and security problems latent in electronic health records. Specifically, this Note discusses HIPAA and HITECH, the current law in place, and how blockchain technology can be used to fix the accessibility and security problems of current electronic health records. This Note proposes that blockchain technology can help a healthcare industry struggling to adhere to the current rule of law in an era of Big Data. Further, Blockchain technology can help individual consumers, particularly those with significant health issues, obtain the best possible medical care while simultaneously keeping their private and sensitive information safe. This innovative technology offers the security and sophistication needed to usher healthcare providers and healthcare consumers into a new technological era fraught with privacy issues.

Table of Contents

I. Introduction 288

II. Overview of the History of Electronic Health Care Records and Data Privacy 290

III. What is HITECH—Just a New HIPAA? HITECH's Benefits and Burdens 293

IV. What is a Blockchain—the Truth Ledger 300

---

1. This is a take on "FinTech," or the slang for Financial Technology. The author knows of "FinTech" from conversations with Professor Joshua A.T. Fairfield of Washington & Lee School of Law.

* Candidate for J.D. May 2019, Washington and Lee University School of Law.

V. Practical Uses of Blockchain Technology—from the Banking Industry to the Most Impoverished.....302

VI. Blockchain Pitfalls—Drawbacks of a New Technology 306

VII. How Blockchain Technology Can Change EHRs—"A New Model for Health Information Exchanges." 307

VIII. Conclusion.....312

I. Introduction

Have you been to a doctor's office where they plug your vital signs and information into a computer? Have you used a website to talk to your doctor about refilling prescriptions or to schedule your next appointment? The technological age has brought about changes not only to smartphones but also to the way persons interface with their doctors—this is the age of electronic health records.

While the switch to electronic heath records (EHRs) has important and consequential benefits, switching to EHRs has also presented several difficulties.[2] The most prominent difficulty is the combination of the decentralized information and the amalgamation of different software tools that doctors and healthcare providers use to file their electronic healthcare records.[3] The lack of a centralized tool has made it difficult for doctors and healthcare providers to share information across offices, threatening patient privacy.[4] Many patients justifiably

2. *See* Frank Moss, *Our High-Tech Healthcare Future is Here. But It's Not What I Thought.*, TWINE HEALTH (Jan. 28, 2016), https://www.twinehealth.com/blog/our-high-tech-healthcare-future-is-here.-but-its-not-what-i-thought (discussing the future of healthcare and electronic healthcare records) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

3. *See id.* (discussing latent difficulties in the adoption of electronic healthcare records and the struggle of healthcare providers to find and use appropriate EHR software).

4. *See Why Hackers Are Increasingly Targeting Electronic Health Records*, TREND MICRO (Apr. 3, 2017), http://blog.trendmicro.com/why-hackers-are-increasingly-targeting-electronic-health-records/ (discussing latent issues with electronic healthcare records and why those issues make electronic healthcare

worry that their information will be "hacked."[5] In 2016 alone, "on average, at least one health data breach occurred every day."[6] Hackers prey on health records because it is easy for them to access the fragmented and "siloed" systems.[7] At the same time, because healthcare providers are legally required to provide EHRs,[8] many are stuck with systems that leave patients open to data and privacy threats.[9]

The possible solution lies in a modern technological innovation that changes the way transactions occur on a daily basis—blockchain.[10] Summed up, a "'blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything else.'"[11] By tracking data in a fashion that also protects informational privacy,[12] Blockchain technology could be the key to fixing the inherent failings of the current software systems housing EHRs.

---

records softer targets for data hackers) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also* Lynda C. Burton, Gerard F. Anderson, & Irvin W. Kues, *Using Electronic Health Records to Help Coordinate Care*, 82 MILBANK Q. 457, 460 (2004) (discussing the "barriers to widespread adoption" of electronic health care records).

5. *See Why Hackers Are Increasingly Targeting Electronic Health Records*, *supra* note 4 (discussing latent issues with electronic healthcare records and why those issues make electronic healthcare records softer targets for data hackers).

6. *Id.*

7. *See id.* (discussing why the issues with electronic healthcare records make them easy targets for data hackers).

8. *See* Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 115-231 (codified in scattered sections of 42 U.S.C.) (2009) (stipulating the legal requirements for electronic health care records and healthcare providers).

9. *See Why Hackers are Increasingly Targeting Electronic Health Records*, *supra* note 4 (discussing latent issues with electronic health care records and why those issues make electronic healthcare records softer targets for data hackers).

10. *See* Ameer Rosic, *What is Blockchain Technology?* BLOCKGEEKS, https://blockgeeks.com/guides/what-is-blockchain-technology/ (last visited Nov. 3, 2018) (discussing the fundamental characteristics of blockchain technology) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

11. *See id.* (discussing the fundamental characteristics of blockchain technology).

12. *Blockchain 101 Infographic*, IBM, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XI912346USEN& (last visited Nov. 3, 2018) (citing Don & Alex Tapscott, the authors of *Blockchain Revolution*) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

II. Overview of the History of Electronic Health Care Records and Data Privacy

By definition, an EHR is "'a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports.'"[13] EHR systems store an individual's records in a single location for a particular health care provider, so that doctors and nurses can access up-to-date information at later dates.[14] There are many benefits to using EHRs: EHRs, if implemented correctly, (1) allow doctors to communicate across offices about patient specific issues; (2) make it easier for doctors to track patient care; and (3) save time, which can be critical in emergency situations.[15]

Starting as early as the late nineties and early 2000s, private individual healthcare providers started recognizing the benefits of EHRs and, accordingly, began using EHRs in their practices.[16] For example, in 2003, "a number of well-known health systems and academic medical centers, such as the LDS Hospital in Salt Lake City and Brigham Women's Hospital in Boston . . . developed their own integrated electronic clinical record system."[17]

The federal government has also started to take notice of EHRs.[18] For instance, in 2003 the Agency for Health Care

---

13. Nir Menachemi & Taleah H. Collum, *Benefits and Drawbacks of Electronic Health Record Systems*, 4 RISK MGMT. HEALTH POL'Y 47, 48 (2011) (citing the definition of EHRs provided by the Healthcare Information and Management Systems Society).

14. Burton, Anderson, & Kues, *supra* note 4, at 458.

15. *See Benefits of Electronic Health Records*, UNIV. OF S. FLA., https://www.usfhealthonline.com/resources/healthcare/benefits-of-ehr/ (last visited Nov. 3, 2018) (giving an in-depth discussion of what EHRs are, who uses them, and their relevant benefits) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

16. *See* Burton, Anderson, & Kues, *supra* note 4, at 467 (detailing the history of the development of electronic healthcare records and why players started to take notice of EHRs).

17. *Id.*

18. *See id.* at 470 (describing the federal government's historical involvement in electronic health records and why they started to take notice of EHRs).

Research and Quality (AHRQ), "the leading federal agency in supporting research on information technology," awarded fifty million dollars in grants to "support organizational and community-wide implementation and diffusion of health information technology . . . ."[19] Similarly, the federal government also relies on "highly developed integrated electronic clinical data systems in the Veterans Health Administration (VHA) and the U.S. Department of Defense."[20]

EHRs were first alluded to in government regulations in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[21] References to electronic records appear most notably in title II, subtitle F of HIPPA—"Administrative Simplification."[22] There, it states that the purpose of HIPAA is to improve "the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the *electronic transmission of certain health information*."[23] HIPAA, however, primarily describes how to keep patient medical information private rather than the EHRs themselves.[24]

The Federal Government first introduced the importance of widespread EHR use as part of the American Recovery and Reinvestment Act of 2009 (Recovery Act).[25] The Recovery Act was implemented following the economic recession of 2008 as a way to stimulate the economy.[26] Among several enumerated goals, the Recovery Act aims to "provide [the] investments needed to increase economic efficiency by spurring technological advances in science

---

19. *Id.*

20. *Id.*

21. *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-91, 110 Stat. 1936 (1996) (establishing statutory guidance on healthcare information compliance).

22. *Id.* § 262.

23. *Id.* (emphasis added).

24. *See id.* (stipulating rules on informational privacy).

25. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (codified in scattered sections of 42 U.S.C.).

26. *See Overview of the American Recovery and Reinvestment Act of 2009 (Recovery Act)*, U.S. TREASURY, https://www.treasury.gov/tigta/recovery.shtml (last visited Nov. 3, 2018) (describing the reasons for the Recovery Act and its basic provisions) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

and health."[27] To achieve this goal, the Recovery Act calls for the implementation of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[28] HITECH amended the Public Service Act to "establish[] within the Department of Health and Human Services an Office of the National Coordinator for Health Information Technology."[29] The National Coordinator's would oversee the "development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information . . . ."[30] To achieve this task, HITECH amended the Public Health Service Act to ensure (1) "the electronic exchange and use of health information and the enterprise integration of such information[]"[31] and (2) "[t]he utilization of an electronic health record for each person in the United States by 2014."[32] HITECH also imposes EHR adoption incentives for Medicare and Medicaid as well as "penalties on those who refuse[] or fail[] to adopt or implement EHR systems."[33] Thus, the federal government created HITECH to help usher the healthcare industry into the modern technological era.[34] Although HITECH did not solve every problem for healthcare providers and patients, its adoption signaled the dawn of widespread use of EHRs.[35]

---

27. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, §3(a)(3), 123 Stat. 115, 116 (codified in scattered sections of 16 U.S.C., 42 U.S.C.).

28. *See id.* §13001 (describing HITECH and its role in implementing electronic health records).

29. *Id.* §13101.

30. *Id.*

31. *Id.*

32. *Id.*

33. *See* Jenny Carroll & Daniel O. Carroll, *Electronic Health Records*, 299 APR N.J.L. 55, 57 (describing the implementation scheme of HITECH).

34. *See id.* at 55 (describing the history of the implementation of HITECH and electronic health care records and the importance of HITECH's implementation scheme).

35. *See id.* at 61. (same).

III. What is HITECH—Just a New HIPAA? HITECH's Benefits and Burdens

HITECH goes well beyond HIPAA in ensuring the development of widespread EHR use. HITECH offers a complex implementation scheme in order to ensure health care providers switch over to EHRs.[36] Primarily, HITECH lays the foundation for a government-sponsored EHR incentive program: "[T]o receive incentive payments . . . providers must be eligible and must successfully demonstrate meaningful use of EHRs for each year of participation in the EHR incentive program."[37] Beyond these requirements, HITECH "relies on [Centers for Medicare and Medicaid Services] (CMS) to promulgate regulatory requirements to determine how and when providers achieve 'meaningful use' of certified EHRs."[38] In its efforts, CMS has adopted a "staging" strategy in order to "phase in the requirements for EHR adoption and meaningful use over time in successive stages."[39] The staging breaks down in the following ways: (1) Stage One—the "meaningful use criteria is focused on data capture and sharing";[40] (2) Stage Two—the "meaningful use criteria is focused on advance[d] clinical processes";[41] and (3) Stage Three—the "meaningful use criteria is focused on improved outcomes . . . ."[42]

Healthcare providers that comply with the stages receive incentive payments, while those who do not become "subject to penalties of payment adjustments."[43] The staging process offers health care providers the ability to gradually adopt EHRs in a way that "maintain[s] flexibility with ever-changing and rapidly developing HER technology . . . ."[44] Accordingly, the staging strategy "allow[s] rulemaking based on user experience with the

---

36. *See* Carroll & Carroll, *supra* note 33, at 57 (describing the basics of HITECH).

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

42. *Id.* Carroll & Carroll, supra note 33, at 57.

43. *Id.*

44. *See id.* (describing the staging period in detail and its benefits to healthcare providers).

available technology, [with] each stage . . . progressively and incrementally expand[ing] the requirements for achieving meaningful use of EHRs."[45] Thus, no healthcare provider is rushed into adopting an overly complex and incomprehensive EHR system.[46]

Nevertheless, HITECH and CMS's regulatory staging fails to account for the realities of EHR implementation in practice. As mentioned in their article, *Electronic Health Care Records*,[47] legal scholars Jenny Carroll and Daniel O. Carroll reviewed several studies on the "real world (i.e., non-legal) challenges for healthcare providers adopting and implementing EHR systems."[48] They divided the challenges into three categories: "[(]1) [C]ost; [(]2) technical issues; and [(]3) workforce training and education."[49]

Healthcare providers sustain substantial costs to purchase and install EHR systems.[50] Implementing an EHR system can "cost a single physician approximately $163,765."[51] Furthermore, many healthcare providers must bear this cost until they can show CMS that their EHR system meets the "meaningful use" standard.[52] Those who cannot afford the initial cost of an EHR system face "financial penalties for not meeting the new standards" under Hitech and CMS regulations.[53] Thus, the

---

45. *Id.*

46. *See id.* (describing the basics of HITECH implementation and the benefits of the staging process to health care providers).

47. *See id.* (describing the basics of HITECH).

48. Carroll & Carroll, *supra* note 33, at 58.

49. *See id.* (explaining that after they reviewed several studies, the authors categorized the main challenges presented to healthcare providers in implementing EHR systems).

50. *See id.* (detailing the specifics of each stipulated category).

51. Tara O'Neill Hayes, *Are Electronic Medical Records Worth the Costs of Implementation*, AM. ACTION F. (Aug. 6, 2015), https://www.americanactionforum.org/research/are-electronic-medical-records-worth-the-costs-of-implementation/ (quoting Neil S. Fleming, *Exploring Financial and Non-Financial Costs and Benefits of Health Information Technology*) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

52. *See id.* (describing the issues with implementing EHR systems and the costs of implementing such systems as a burden on health care providers).

53. *Id.* Nevertheless, O'Neill Hayes notes that "[p]roviders are allowed to apply for a hardship exemption if [they are] unable to meet the criteria; if approved, these providers would not be penalized." *Id.* n.7.

regulatory scheme puts providers in a Catch-22: Pay for EHR implementation or pay a penalty.

Healthcare providers must also remain vigilant of technical problems that could hamper their ability to comply with HITECH.[54] For example, healthcare providers have to choose EHR systems that address "technical concerns, such as system interoperability (*i.e.,* healthcare data maintained in 'silos'), non-standardized EHR applications, concerns about privacy and security, risks of technical errors[,]"[55] and many other issues. Healthcare providers essentially have to "shop" for software that meets their EHR needs.[56] Is the government, then, asking our doctors to become technical software experts?

Any EHR implementation also requires extensive employee training.[57] Think of nurses inputting your data into a computer when they take your vitals. Like with any new technology, human users need help to understand a software's basic functions. But, extensive employee training means more costs: Costs to train and costs associated with interruptions in daily workflow.[58] If the training is not successful, human error and poorly trained employees can "threaten a successful launch and the healthcare provider's substantial investment of time and money."[59] Add training and workflow interruption to the growing list of EHR implementation issues.

Healthcare providers must also comply with guidelines and standards under HIPAA and HITECH that offer little help in actually choosing appropriate software to safeguard protected information. HIPAA was enacted to ensure that patients "have rights over [their] own health information, no matter what form it is in."[60] More specifically, "Congress recognized the need to

---

54. *See* Carroll & Carroll, *supra* note 33, at 58 (describing what healthcare providers need to do in order to implement EHRs and comply with HITECH).

55. *Id.*

56. *See id.* (describing the role of healthcare providers in EHR implementation).

57. *See* Carroll & Carroll, *supra* note 33, at 58 (describing what healthcare providers need to do in order to implement EHRs and comply with HITECH).

58. *Id.*

59. *Id.*

60. OFF. FOR C.R., PRIVACY, SECURITY, AND HEALTH RECORDS 2, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf (on file with the Washington & Lee

maintain strict privacy protection for Protected Health Information (PHI) and therefore authorized the Department of Health and Human Services to promulgate regulations . . . known collectively as the Privacy Rule."[61] The Privacy Rule has four main objectives: (1) To "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information[;]"[62] (2) to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information[;]"[63] (3) to "[p]rotect against any reasonably anticipated uses or disclosures of such information that are not permitted[;]"[64] and (4) to "[e]nsure compliance with this subpart by its workforce."[65] The Privacy Rule applies to any HIPAA "covered entities" which includes any healthcare provider who, regardless of size,[66] "transmits any health information in electronic form in connection with a transaction covered by [HIPAA]."[67] HIPAA, however, does little to provide specific guidance to covered providers as to the best way to safeguard data.[68] HIPAA merely gives vague guidelines such as, "[a] covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information."[69] But, what is "reasonable and appropriate?" Healthcare providers are left alone to determine which software will comply with HIPAA's complicated Privacy Rule.

Journal of Civil Rights & Social Justice).

61. *Id.*; *see* Standards for Privacy of Individually Identifiable Information, 66 Fed. Reg. 12,434 (Feb. 26, 2001) (to be codified at 45 C.F.R. pt. 160, 164) (articulating the "Standards for Privacy of Individually Identifiable Health Information.").

62. 45 C.F.R. § 164.306(a)(1) (2018).

63. *Id.* § 164.306(a)(2).

64. *Id.* § 164.306(a)(3).

65. *Id.* § 164.306(a)(4).

66. *See* U.S. DEP'T OF HEALTH & HUM. SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE 2 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf (providing an overview of the HIPPA privacy rule) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

67. *Id.* § 160.103.

68. *See id.* pt. 160, 165 (failing to provide guidance on protecting data).

69. U.S. DEP'T OF HEALTH & HUM. SERVICES, *supra* note 66, at 14.

What about HITECH? HITECH is essentially an extension of HIPAA's privacy protections. HITECH "increases the scope of privacy and security protections available under HIPAA[] [and] increases potential legal liability for non-compliance and provides more enforcement of HIPAA rules."[70] In tandem, HIPAA and HITECH impose significant penalties on these providers who violate the PHI regulations and the Privacy Rule.[71] Since the enactment of HIPAA and HITECH, there have been over 20,000 compliance investigations among healthcare providers.[72] Among the top three compliance issues cited in these investigations was "[l]ack of administrative safeguards of electronic PHI."[73] Penalties for these breaches "can bring fines as high as $50,000 per violation and up to $1.5 Million per year."[74] Thus, healthcare providers receive little concrete guidance on how to comply, while simultaneously becoming subject to severe penalties for noncompliance. Beyond government penalties, data breaches themselves cost health care providers significant amounts. At $398 per comprised record, the average cost of data breaches in the healthcare industry is more expensive than the $217 per compromised record for standard breaches in other industries.[75] Non-compliance means that healthcare providers could be hit twice with increased costs.

---

70. *See* Jason Juliano, *HIPAA HITECH and Big Data Privacy Concerns*, LINKEDIN (Mar. 12, 2014), https://www.linkedin.com/pulse/hipaa-hitech-big-data-privacy-concerns-jason-juliano (identifying problems with HIPAA and HITECH) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

71. *See id.* (describing issues of non-compliance).

72. *See id.* (same).

73. *Id.*

74. *Id.*

75. *See* SPRINKLR, HOW TO CALCULATE THE COST OF A DATA BREACH 3 (2015), https://blog.sprinklr.com/wp-content/uploads/securepdfs/2016/03/20161125_WP_EN_How_to_Calculate_the_Cost_of_a_Data_Breach_Updated_V01.pdf (providing estimates of data breach costs across industries) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also* Elizabeth Snell, *Healthcare Data Breaches Have Highest Cost, Says Ponemon*, HEALTHITSECURITY (May 27, 2015), https://healthitsecurity.com/news/healthcare-data-breaches-have-highest-cost-says-ponemon (same) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

In an effort to keep themselves compliant, some providers hire compliance officers.[76] These compliance officers, however, come at a price. According to the U.S. Bureau of Labor Statistics, compliance officers can make upwards of $70,000.[77] This added expense, in combination with the costs of the software itself, training, and potential penalties makes HER implementation difficult and costly.

HIPAA and HITECH purport to ensure EHR implementation by incentivizing providers to not only adopt EHRs, but also keep records safe and confidential.[78] Nevertheless, these regulations seemingly do nothing more than police. They only offer rules to follow and the penalties to pay when rules are broken.[79] They offer little guidance to help providers navigate the complicated world of technology.[80] As a result, providers implement expensive technology their employees know little about.[81] Furthermore, as Big Data increases, it becomes harder and harder to oversee and manage the security of healthcare records.[82] HITECH's policing does not account for healthcare providers who make good faith

---

76. *See* Ryan Black, *No One Is Sure Why Amazon Needs a HIPAA Compliance Officer*, HEALTHCARE ANALYTICS NEWS (Jan. 16, 2018), http://www.hcanews.com/news/no-one-is-sure-why-amazon-needs-a-hipaa-compliance-officer (detailing how more and more companies are hiring compliance officers and how compliance officers can help businesses follow healthcare regulation) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

77. *Occupational Employment and Wages, May 2017: 13-1041 Compliance Officers*, U.S. BUREAU OF LAB. STAT., https://www.bls.gov/oes/current/oes131041.htm (last visited Feb. 22, 2018) (providing the national salary estimates for compliance officers) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

78. *See* Carroll & Carroll, *supra* note 33, at 56, 60 (explaining that after they reviewed several studies, the authors categorized the main challenges presented to healthcare providers in implementing EHR systems).

79. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. (stipulating statutory guidelines for healthcare technology infrastructure); *see also* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-91, 110 Stat. 1936 (stipulating statutory guidelines for privacy in the healthcare industry).

80. *Supra* note 79. (stipulating statutory guidelines but barely discussing how to implement them).

81. *See* Carroll & Carroll, *supra* note 33, at 58 (describing the pressing need to train employees in EHR software).

82. *See* Juliano, *supra* note 70 (noting the natural consequences of implementing complicated EHR software).

efforts to comply with HITECH but nevertheless have understandable troubles finding effective data solutions. Such incomplete regulations leave many electronic health records—and patients—at risk.

Many patients have suffered the consequences, and will continue to suffer the consequences, inherent in the current EHR systems used by healthcare providers. Chief among the risks to individual healthcare consumers is general patient safety.[83] Because many healthcare providers use data management systems in silos, it is very difficult for providers to communicate with one another about patient care.[84] For patients with extensive and inter-related health issues, this can lead to serious hazards such as medication mistakes and allergy risks.[85] For example, in an incident described in a report by the U.S. Department of Veterans Affairs' Informatics Patient Safety Office, an emergency department doctor prescribed a patient medication that she was allergic to because a network problem with the EHR system prevented the doctor from remotely accessing the patient's listed allergies.[86] These are just some of the host of concerns plaguing patients under current EHR systems.

As many scholars posit, what is needed is a solution that can "handle both storage and management of large amounts of data[]"[87] in a centralized location that allows cross pollination of information with other providers, while simultaneously maintaining the privacy and integrity of the data involved.[88] Well, what about a blockchain?

---

83. *See* M.W. Meeks et al., *An Analysis of Electronic Health Record-Related Patient Safety Concerns*, U.S. NAT'L LIBR. OF MED. (2014) (observing and investigating patient safety concerns related to electronic medical records concluding that "institutions with long-standing as well as recent EHR implementations should build a robust infrastructure to monitor and learn from them.").

84. *See* Carroll & Carroll, *supra* note 33, at 60 ("Rather than one physician's office calling another to request medical records, or faxing a consent to do so, providers can now pull or push data from an online portal containing information compiled by multiple specialists and providers.").

85. *See* Meeks, *supra* note 83 (providing examples of hidden dependencies in current EHR systems).

86. *See id.* (same).

87. *See* Juliano, *supra* note 70 (explaining the effects of healthcare law on a healthcare industry grappling both with Big Data and compliance issues).

88. *See id.* (same).

IV. What is a Blockchain—the Truth Ledger[89]

When most people hear the word blockchain, they associate it with the ever-popular cryptocurrency, BitCoin.[90] Blockchain is the technology *behind* BitCoin and, more importantly, has aggressively expanded beyond the economic sectors that deal with cryptocurrency.[91] A blockchain is "a database or ledger that maintains a continuously growing list of data records or transactions."[92] Blockchain thus refers to multiple blockchains that can be used by various actors, rather than just one universal blockchain. Blockchains are essentially sophisticated versions of excel spreadsheets.[93] Blockchain technology, however, has some key qualities beyond traditional excel spreadsheets which may be helpful to healthcare providers and EHR implementation.

Blockchains are generally "shared publically."[94] This does not mean that your law professor can access a blockchain and see the medical history recorded within. Rather, in a private blockchain,[95] information is shared publically among the specific "nodes,"[96] or

---

89. Nickname for Blockchain from Professor Josh Fairfield of Washington & Lee University School of Law. This section will only cover the basics of blockchain technology for the reader.

90. *See* Portia Crowe, *There is a 'Game Changer' Technology on Wall Street and People Keep Confusing It with Bitcoin,* BUS. INSIDER (Mar. 5, 2016), http://www.businessinsider.com/what-is-blockchain-2016-3 (explaining the differences between BitCoin and blockchain and describing the essential characteristics of the Blockchain) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

91. *See id.* (same).

92. *See* Alexia Jengten, *Cryptosphere—Unraveling the Mystery Part I: Blockchain: A Ledger for the Modern Era*, IPOHUB (Sept. 15, 2018), https://www.ipohub.org/cryptosphere-unraveling-the-mystery-part-1-blockchain-a-ledger-for-the-modern-era/ (giving a basic understanding of blockchain and its capabilities) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

93. *See id.* (giving a basic understanding of blockchain and its capabilities).

94. *See id.* (same).

95. *See* Praveen Jayachandran, *The Difference Between Public and Private Blockchain*, IBM, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (last visited on Nov. 4, 2018) (noting the difference between a private and public block chain) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

96. *See* Jengten, *supra* note 92 (defining a node and explaining how a node fits into the overall Blockchain System).

participants,[97] of that block.[98] Accordingly, blockchains are permissioned—they give "each member of the network . . . access rights so that confidential information is shared on a need-to-know basis."[99] The nodes input the information and "maintain the entries (known as blocks) and every node sees the transaction data stored in the blocks when created."[100] This means various participants can see data that other participants entered.[101] Thus, a blockchain "works as a shared system of record among participants on a business network, eliminating the need to reconcile disparate ledgers."[102]

Blockchains are also considered secure.[103] This is because "the ledgers and underlying databases are immutable and irreversible."[104] In other words, "posts to the ledger cannot be revised or tampered with . . . ."[105] Blockchains use cryptography[106]

---

97. An example of a "participant in the ledger" for these purposes would be one healthcare provider among a group of other "nodes" or other healthcare providers.

98. *See* Jengten, *supra* note 92 (explaining the basic structure of a blockchain).

99. *Blockchain 101 Infographic*, *supra* note 12.

100. Jason Bainter, *The Smoke Detector: Do You Know How Blockain Is Chaging Business?*, CPA CTR. OF EXCELLENCE (Mar. 7, 2017), http://cpacoe.incpas.org/blogs/jason-bainter/2017/03/07/the-smoke-detector-do-you-know-how-blockchain-is-changing-business (on file with the Washington & Lee Journal of Civil Rights).

101. *See* Jengten, *supra* note 92 ("All nodes within a network have complete, unfettered access to the ledger because each node has a complete copy of the ledger on its server.")

102. *Blockchain 101 Infographic*, *supra* note 12.

103. *See id.* (explaining that changes to a blockchain require consensus "from all network members, and [that] all validated transactions are permanently recorded. No one, not even a system administrator, can delete a transaction.").

104. Bainter, *supra* note 100; *see* Nitin Anand, *Applications of Blockchain in FinTech*, MEDIUM (Aug. 6, 2018), https://medium.com/futrtec/applications-of-blockchain-in-fintech-86b3c8c3a5ab (describing the fundamental characteristics of blockchain) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

105. Anand, *supra* note 104.

106. For an in depth look at cryptography see Gary C. Kessler, *An Overview of Cryptography*, GARYKRESSLER.NET (Aug. 11, 2018), https://www.garykessler.net/library/crypto.html (providing the basic concepts of cryptography) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

to both verify these ledger posts and keep them secure.[107] Cryptography essentially encrypts data to prevent those outside of a permissioned chain from gaining access to the data recorded within.[108] Finally, Blockchain is automated: "The software is written so that conflicting or double transactions do not become written in the data set and transactions occur automatically."[109] Thus, a blockchain is essentially a ledger that collects and keeps track of data automatically.[110] But, how is blockchain technology already useful in real world transactions? Case studies by the banking industry, the government, and many others demonstrate just how useful blockchain technology can be.

V. Practical Uses of Blockchain Technology—From the Banking Industry to the Most Impoverished

Blockchains are used and can be used in a host of different economic sectors. Specifically, Blockchain use has recently increased among players in the banking industry.[111] Ripple, a blockchain provider, has been on the forefront of the blockchain movement, "enable[ing] banks to transact directly with each other and lower[ing] the total costs of settlement." [112] Ripple's pitch to banking institutions is that "[b]y joining [their] growing, global network, financial institutions can process their customers' payments anywhere in the world instantly, reliably and cost-effectively."[113] Ripple and Ripple's blockchain have been the center of a plethora of transactions and projects between banks.[114]

---

107. *See id.* (same).

108. *See id.* (same).

109. Anand, *supra* note 104.

110. *Blockchain 101 Infographic*, *supra* note 12.

111. *See* John Manning, *How Blockchain is Changing the Banking Industry*, INT'L BANKER (Sept. 4, 2017), https://internationalbanker.com /banking/blockchain-changing-banking-industry (describing the increase in blockchain use in the realm of financial technology) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

112. *See id.* (noting companies providing blockchain services).

113. *See Our Company*, RIPPLE, https://ripple.com/company/ (last visited Nov. 4, 2018) (describing Ripple and what they can do for banking institutions) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

114. *See* Manning, *supra* note 111 (describing increasing blockchain use in

For example, Ripple's blockchain is used to power an instant-remittance service[115] for use between banks in Japan and Thailand.[116] Using blockchain in this manner helps Japanese and Thai banks "boost the speed, efficiency and cost of the countries' remittance corridor, which sees around $250 million transferred every year, largely as a result of the 40,000 Thai nationals living in Japan."[117] Furthermore, a host of prominent international banks—including Barclays, HSBC, Deutsche Bank, and others—have banded together to use Ripple's chain to create "the utility settlement coin."[118] The coin is "a digital currency that will primarily be used to quickly clear and settle financial transactions . . . to reduce the time, cost and capital required for the post-trade clearing and settlement process, as well as to improve financial-market efficiency."[119]

Blockchain technology is also useful in supply chain interactions.[120] Blockchains work well in supply chain interactions because they enable "proof of ownership and the transfer of ownership from one entity to another without using a trusted third party intermediary (like a bank)."[121] Moreover, the various transactions between parties in the supply chain are fully recorded on the blockchains, allowing parties to verify transaction information.[122] Companies, such as T-mining, for example,

---

the financial technology sector).

115. An instant-remittance service is a service used to instantly send money between parties. *See Remit*, FREE DICTIONARY, https://financial-dictionary.thefreedictionary.com/remitter (last visited Nov. 4, 2018) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

116. *See* Manning, *supra* note 111 (describing increasing blockchain use in the financial technology sector).

117. *Id.*

118. *Id.* Other lending institutions that have joined this effort include Credit Suisse, Canadian Imperial Bank of Commerce, MUFG (Mitsubishi UFJ Financial Group), State Street, Banco Santander, Bank of New York Mellon, and NEX. *Id.*

119. *Id.*

120. *See* Steve Banker, *Blockchain In The Supply Chain: Too Much Hype*, FORBES (Sept. 1, 2017), https://www.forbes.com/sites/stevebanker/2017/09/01/blockchain-in-the-supply-chain-too-much-hype/#124e16f198c8 (describing the plethora of uses for blockchain in the supply chain) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

121. *Id.*

122. *See id.* (describing the plethora of uses for blockchain in the supply

specifically use a blockchain to verify shipments between parties.[123] Blockchain technology works well in this context because it acts as a "digital distributed ledger [that] create[s] a single electronic place where all the myriad documents related to a shipment . . . [are] housed."[124] The security of blockchain technology also cuts down on the number of "fictitious pickups"[125] that increasingly plague supply chain industries.[126]

Beyond businessmen and profit-seekers, governments and nonprofits use blockchains to help impoverished people in the United States and across the world.[127] In May 2017, the United Nations, Parity Technologies,[128] and Datarella,[129] worked together to implement the United Nation's World Food Programme (WFP) blockchain.[130] The Programme gave Syrian refugees cryptocurrency-based vouchers that were used to purchase food items.[131] The blockchain platform was "successfully used to record

---

chain).

123. *See id.* (same).

124. *Id.*

125. *See id.* ("[Fictitious pickups] occur when con artists show up at a shipper's dock, provide fabricated insurance documents, DOT numbers for trucks, and pickup documentation.").

126. *See id.* (describing blockchain's responsiveness to an industry-specific problem).

127. *See* Quora, *What Is Blockchain Used for Besides Bitcoin*, FORBES (Nov. 17, 2017), https://www.forbes.com/sites/quora/2017/11/17/what-is-blockchain-used-for-besides-bitcoin/#5a0373d3446e (describing situations where nonprofits and governmental bodies have used blockchain to provide aid for impoverished and hungry people) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

128. Parity Technologies is a blockchain infrastructure startup based in London, UK. *See About Parity Technologies*, PARITY, https://www.parity.io/about/ (last visited Nov. 4, 2018) (describing Parity Technologies) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

129. Datarella is a German-based blockchain provider. *See Imprint*, DATARELLA, https://datarella.com/imprint-2/ (last visited Nov. 4, 2018) (identifying Datarella's headquarters in Munich, Germany) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

130. *See* Michael del Castillo, *United Nations Sends Aid to 10,000 Syrian Refugees Using Ethereum Blockchain*, COINDESK (June 13, 2017), https://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/ (reporting on the World Food Programme) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

131. *See id.* (same).

and authenticate transfers for about 10,000 individuals."[132] The success of the program has led to an expansion that will seek to achieve "Zero Hunger by 2030."[133]

Innovators and business organizations recognize the importance of blockchain technology in other sectors of the economy as well. For example, food distributors are looking to potentially use blockchain technology to help "establish the authenticity of food."[134] IBM is exploring blockchain's use in "food traceability, and has [accordingly] announced a consortium with several major food producers and retailers [to delve into the subject]."[135] Some are even looking into using blockchains to protect against voter fraud.[136] The startup Follow My Vote plans to use the emerging technology to cut down on voter fraud.[137] Blockchain technology "has the ability to provide an unhackable electronic vote-counting system . . . [that] can secure an election during voter registration, . . . account for the voters identification[,] and insure [that] votes cannot be tampered with at a later date."[138] A blockchain would act as a "permanent and public ledger for votes as tallied—promising a future of equitable democratic election around the world."[139] Blockchain technology has many potential uses still to be explored.

---

132. *Id.*

133. *Id.*; *see Zero Hunger Challenge*, U.N., http://www.un.org/en/zerohunger/challenge.shtml (last visited Feb. 21, 2018) (detailing the United Nations Zero Hunger Challenge in "Transforming our Foods System to Transform our World") (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

134. *See* Banker, *supra* note 120 (describing the different commercial uses for blockchain).

135. *Id.*

136. *See* Quora, *supra* note 127 (discussing the democratic potential of Blockchain).

137. *See How We Can All Stop Voter Fraud*, FOLLOWMYVOTE.COM, https://followmyvote.com/can-stop-voter-fraud/ (last visited Nov. 4, 2018) (describing the general idea behind Follow my Vote) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also* Quora, *supra* note 127 (discussing Follow My Vote and other startups looking into Blockchain for uses beyond Bitcoin).

138. Quora, *supra* note 127.

139. *Id.*

VI. Blockchain Pitfalls—Drawbacks of a New Technology

Despite the many successful and potential uses of blockchain technology, it nevertheless comes with some drawbacks.[140] Blockchain technology development has fallen to a relatively small number of companies, and the majority of these are startups.[141] As a result, individual developers of the technology—the human element—are "scarce and expensive."[142] Moreover, some blockchains that were "near-free" now feature "notable transaction costs."[143] Companies must pay blockchain providers like Ripple to help them do business, while also bearing additional per transaction costs that can reach approximately $0.20.[144] Although such a cost may seem insignificant, the sheer volume of transactions can quickly add up to large amounts.[145]

Furthermore, because blockchain technology is new, many still do not use it.[146] The lack of commercial blockchain users inhibits the potential of the technology as a viable business tool—for blockchain to be effective, all parties in a business transaction must adopt it.[147] For example, in a supply chain transaction, all parts of that supply chain—from manufacturer, to delivery service, to distributor—must use the blockchain:[148] "If a blockchain is not a robust network with a widely distributed grid of nodes, it becomes more difficult to reap the full benefit."[149]

---

140. *See* Banker, *supra* note 120 (describing the beneficial uses of Blockchain while keeping in mind its potential difficulties).

141. *See id.* (describing the history of blockchain usage and what blockchain usage looks like today).

142. *See id.* (same).

143. *See What Are Blockchain's Issues and Limitations*, COINDESK, https://www.coindesk.com/information/blockchains-issues-limitations/ (last visited Nov. 4, 2018) (identifying the potential pitfalls of Blockchain) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

144. *Id.*

145. *See id.* (describing the potential limits to using blockchain technology).

146. *See* Banker, *supra* note 120 (describing a specific shortcoming of blockchain).

147. *See id.* (describing a practical problem of blockchain that, in turn, leads to other problems).

148. *See id.* (explaining what is required for a blockchain to function effectively).

149. *What Are Blockchain's Issues and Limitations*, *supra* note 143.

Finally, blockchain is, simply, complicated.[150] Understanding nodes, cryptography, and blocks may be difficult for first-time users or perspective buyers.[151] Also, like with other information databases that rely on user input, human-error can cause problems that blockchain ledgers cannot automatically fix.[152] Thus, although ripe with benefits, there are some drawbacks to blockchain usage.

VII. How Blockchain Technology Can Change EHRs—"A New Model for Health Information Exchanges."[153]

The Office of the National Coordinator for Health Information issued a Technology Interoperability Roadmap that "define[d] critical policy and technical components needed for nationwide [EHR] interoperability [under HITECH] . . . ."[154] The three main components of the Roadmap include (1) "[u]biquitous, secure network infrastructure[;]" (2) "[v]erifiable identity and authentication of all participants[;]" and (3) "[c]onsistent representation of authorization to access electronic health information, and several other requirements."[155] Accordingly, the inherent characteristics of Blockchain technology uniquely lend themselves to addressing these regulatory requirements[156] as well as the two other issues that plague healthcare providers: "(1) [C]ost; [and] (2) technical issues . . . ."[157]

---

150. *See id.* (describing the potential limitations of blockchain technology).

151. *See id.* (same).

152. *See id.* (same).

153. *See Blockchain: Opportunities for Health Care,* DELOITTE, https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html (last visited Nov. 4, 2018) (describing how blockchain might help the healthcare sector) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

154. *See id.* (quoting the Office of the National Coordinator for Health Information Technology).

155. *See id.* (discussing the requirements for effective EHR operation set forth in the roadmap).

156. *See id.* (same).

157. Carroll, *supra* note 33, at 58.

Permissioned blocks[158] offer medical providers one central location to speak with other authenticated medical providers and thus cure the silo effects of the current systems in place.[159] For example, Medical Provider X and Medical Provider Y are both nodes on a permissioned block.[160] X and Y have a patient in common that they jointly treat for a serious disease.[161] Under current EHR systems, if X and Y did not use the same software or system, it would be difficult for them to share information about the patient with each other.[162] In fact, the decentralization of information could lead to duplicates in electronic medical records that could then lead to mistakes in treating the patient.[163] This would defeat one of the government's purposes for EHR implementation: The efficient sharing of patient information across offices to ensure better care.[164] But, by using a blockchain, X and Y can see (1) that they are authenticated and permissioned users on the block as well as (2) all of the pertinent and important information on the block.[165] Thus, "[c]apitalizing on this technology has the potential to connect fragmented systems to generate insights and to better assess the value of care."[166] Thus, blockchain integrated EHRs may help decrease the risk of medication mix-ups and allergy threats.

---

158. *See Blockchain 101 Infographic*, *supra* note 12 (giving a basic understanding of blockchain and its capabilities).

159. *See Blockchain: Opportunities for Health Care*, *supra* note 153 (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).

160. *See* Jengten, *supra* note 92 (describing nodes in a blockchain).

161. So, for example, think of a general practitioner who is working with a specialist.

162. *See* Menachemi, *supra* note 13, at 50 (explaining common errors in electronic medical records).

163. *See* Carroll, *supra* note 33, at 56.

164. *See* Menachemi, *supra* note 13, at 52 (describing medical issues that could arise without a properly implemented EHR system); *see also* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (noting that part of the goals of HITECH and the Recovery Act is to promote more efficiency in the healthcare sector).

165. *See Blockchain: Opportunities for Health Care*, *supra* note 153 (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).

166. *See id.* (discussing how Blockchain might benefit healthcare providers implement EHR systems).

Furthermore, because posts on a blockchain cannot be reversed or tampered with, and because Blockchain does not allow duplications in data sets,[167] the risk of EHR information duplication is low.[168] Similarly, "additions and subtractions to the medical record [are] well understood and auditable across organizations."[169] Thus, for example, if healthcare provider X discovered an allergy for a patient that he shares with healthcare provider Y, X would update the record to reflect as much, and Y would easily discover the update, protecting the patient from the associated risk. Under current EHR systems, the risks of wrong, duplicate, or lack of information are an issue. For example, if a hospital patient "ended up being transferred to another hospital, the new hospital may not be able to access data about [his or her] care that was pushed to the first hospital."[170] What if the first hospital gave the patient a drug that could interact negatively with a drug given at the second hospital? Blockchain can address this problem by ensuring data integrity for its users.[171] Again, blockchain technology could significantly protect medical providers and patients from costly mistakes.

Blockchain also greatly increases the security of EHRs[172] and can thus decrease the risks of sensitive information leaks for patients and the costs of data breaches for healthcare providers.[173] As previously mentioned, the current systems in place make it easy

---

167. *See* Crowe, *supra* note 90 (describing the basic characteristics of a blockchain).

168. *See id.* (same).

169. *See* John D. Halamka et al., *The Potential for Blockchain to Transform Electronic Health Records*, HARV. BUS. REV. (Mar. 3, 2017), https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records (giving examples of how blockchain might help the healthcare industry) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

170. *Id.*

171. *See Blockchain: Opportunities for Health Care*, *supra* note 153 (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).

172. *See id.* (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).

173. *See* Carroll, *supra* note 33, at 56 (explaining that after they reviewed several studies, the authors categorized the main challenges presented to healthcare providers in implementing her systems).

for hackers to access sensitive and private patient information.[174] This forces the costs and penalties associated with data breaches onto healthcare providers.[175] If health care providers used blockchain technology instead, data breaches and their associated costs would likely decline.[176]

Blockchain data security is sophisticated and complicated.[177] Each member on a blockchain has a secret private key and a public key.[178] The public key "[i]dentifies the sender and receiver of each transaction[,]" while the private key "acts as a unique signature on the transaction" that encodes sent messages and decodes received messages.[179] In terms of EHRs, this would mean that each patient would have both a public key and a private key to identify them.[180] Both the public key and the private key are encrypted in order to protect a person's information.[181] Having such a key system limits hacking and data security breaches because "the hacker would need to individually hack every single user to obtain unique private keys to access identifiable information of value."[182] Limiting data breaches means costs saved for health care providers and patients.

Many individuals and companies are recognizing the benefits of using blockchains for EHRs and, accordingly, are working to implement the technology. SimplyVital Health is among a number of companies that are working to create a healthcare specific blockchain.[183] With their platform, Health Nexus, SimplyVital

---

174. *See Why Hackers Are Increasingly Targeting Electronic Health Records*, *supra* note 4 (describing why electronic medical records are soft targets for hackers).

175. *See id.*

176. *See Blockchain: Opportunities for Health Care*, *supra* note 153 (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).

177. *See id.* (noting the advantages of blockchain).

178. *See* Jengten, *supra* note 92 ("A message that is encoded with a private key can only be decoded with its paired public key, and vice versa.").

179. *Id.*

180. *Id.*

181. *See id.* (describing the security latent in blockchain).

182. *Blockchain: Opportunities for Health Care*, *supra* note 153.

183. *See* Jesse Damiani, *SimplyVital Health is Using Blockchain to Revolutionize Healthcare*, FORBES (Nov. 6, 2017), https://www.forbes.com/sites/jessedamiani/2017/11/06/simplyvital-health-blockchain-revolutionize-healthcare/#ba9a347880a0 (exploring SimplyVital and

uses blockchain technology to "secure blockchain data storage and transmission,"[184] among members of the healthcare community. The blockchain itself is healthcare specific: SimplyVital ensures compliance with HIPAA and HITECH, allows for physicians and healthcare providers to share information and data with each other, and also allows healthcare providers to work with others across the industry such as pharmacies, insurers, and the like.[185] Thus, SimplyVital gives healthcare providers a specifically tailored and easy option that does not require the latter to act as software experts—companies like SimplyVital act as experts on their behalf.

Yet, although using a blockchain like Health Nexus poses significant benefits for healthcare providers and patients, there are still some drawbacks.[186] Technology like Health Nexus and blockchain in general, as previously mentioned, is still in its early stages.[187] This not only means that the technology is limited and expensive,[188] but also that "it will take decades for blockchain to seep into [the] economic and social infrastructure."[189] This is because blockchain, as a business model, rests on the upheaval of current economic and social infrastructure, not on the simple replacement of one of more aspects of it.[190] Further, for blockchain

---

its business model) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

184. *See Health Nexus*, SIMPLYVITAL, https://tokensale.simplyvitalhealth.com (last visited Nov. 5, 2018) (describing SimplyVital and its new technology, Health Nexus) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

185. *See id.* (describing the benefits of Health Nexus for the healthcare sector).

186. *See What Are Blockchain's Issues and Limitations*, *supra* note 143 (detailing blockchain limitations and how that might affect the potential future use of the technology).

187. *See* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (Jan. 2017), https://hbr.org/2017/01/the-truth-about-blockchain (describing the potential issues with Blockchain and why it is not in widespread use yet) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

188. *See What Are Blockchain's Issues and Limitations*, *supra* note 143 (detailing blockchain limitations and how that might affect the potential future use of the technology).

189. *See* Iansiti, *supra* note 187 (describing why Blockchain is not in widespread use yet).

190. *See id.* (explaining that "blockchain is not a 'disruptive' technology, which

technology to be successful in the healthcare sector, all players in the healthcare sector will have to adopt it. As one scholar put it, "a social network with just one member is of little use; a social network is worthwhile only when many of your own connections have signed on to it."[191] Blockchain then becomes a game of personal choice—who will step up and be the first one to commit?

Blockchain technology also does not solve the costs and burdens of employee education and training as well as human error.[192] If a nurse inputs a patients' information incorrectly, or does not know how to accurately input the patients information, the blockchain will not automatically fix the error.[193] Blockchain technology only corrects duplications or contradicting information.[194] An initial input that does not conflict or duplicate another input will remain in the record.[195] Furthermore, as previously mentioned, blockchain technology is complex and may require additional training and help from a blockchain company, like SimplyVital, to help healthcare providers and employees fully understand and integrate blockchains into their existing records systems.[196] Thus, moving forward, the cost of implementation will likely remain a concern.

VIII. Conclusion

Despite its potential drawbacks, blockchain technology offers a comprehensive system that can help healthcare providers select a EHR management system that not only complies with HIPAA and HITECH, but that also offers healthcare providers efficiency, ease, and relative cost neutralization. Today, healthcare providers

---

can attack a traditional business model with a lower-cost solution . . . [b]lockchain is a *foundational* technology: It has the potential to create new foundations for our economic and social systems." (emphasis in original)).

191. *Id.*

192. *See What Are Blockchain's Issues and Limitations*, *supra* note 143 (detailing blockchain limitations and how that might affect the potential future use of the technology).

193. *See id.* (same).

194. *See id.* (same).

195. *See id.* (same).

196. *See id.* (detailing blockchain limitations and how that might affect the potential future use of the technology).

struggle with various EHR systems that fragment communication between providers.[197] This fragmentation leads to both issues of privacy as well as general safety[198]—how can providers effectively treat if they lack necessary information from other providers? Providers and patients end up suffering the costs of these systems and get no reprieve or help from the government: The government only acts to penalize those who fail to comply instead of educating providers as to the proper path to take.[199] Faced with an impossible dilemma and significant threats to patients, providers need help.

Blockchain technology offers substantial help. It takes care of the "silo" issue, thereby increasing communication between providers and thus reducing cost and liability.[200] It also takes care of privacy concerns with its permissioned chains and key system.[201] The only potential issues with blockchain is its relative complexity and newness.[202] But, hopefully with time, blockchain will become ingrained in the economic infrastructure[203] and its complexity and newness will wane to growing maturity. As many scholars posit, blockchain is not a "panacea"[204] for the healthcare industry but perhaps one day it will be.

---

197. *See* Menachemi, *supra* note 13, at 48 (describing medical issues that could arise without a properly implemented system).

198. *See id.* (same).

199. *See* Carroll, *supra* note 33, at 57 (describing the costs and burdens of EHR systems and why those burdens are significantly affecting healthcare providers).

200. *See Blockchain: Opportunities for Health Care*, *supra* note 153 (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).

201. *See id.* (same).

202. *See* Iansiti, *supra* note 187 (describing the potential issues with Blockchain and why it is not in widespread use yet).

203. *See id.* (describing why Blockchain is not in widespread use yet).

204. *See Blockchain: Opportunities for Health Care*, *supra* note 153 (describing how blockchain's inherent characteristics can cure certain problems in the healthcare sector).