Blockchain in Heathcare Data

DEVON S. CONNOR-GREEN*

INTRODUCTION

Despite having the most expensive healthcare system, the United States ranks last among eleven industrialized countries for health system quality, efficiency, access to care, equity, and healthy lifestyles.[1] Part of the reason that the United States ranks last can be attributed to the low marks on the time and dollars spent dealing with insurance administration, the lack of communication among healthcare providers, and duplicative medical testing.[2] This ranking is dragged down substantially by inefficiencies in our healthcare system.[3] Despite the current state of the healthcare system, new technologies are emerging that have the potential to shift current power structures and redistribute control of personal data back to individuals. The Office of the National Coordinator for Health Information Technology (ONC)[4] envisions a future with:

> [L]earning health systems (LHS),[5] where individuals are at the center of their care; where providers have a seamless ability to securely access and use health information from different sources; where an individual's health information is not limited to what is stored in electronic health records (EHRs), but include information from many different sources (including technologies that individuals use) and portrays a longitudinal picture of their health, not just episodes of care; where diagnostic tests are only repeated when necessary, because the information is readily available; and where public health agencies and researchers can rapidly learn, develop, and deliver cutting edge treatments.[6]

---

* Devon S. Connor-Green earned his Juris Doctor from the University of San Francisco School of Law in May 2017. He earned his B.A. from Evergreen State College in 2007. Devon wishes to thank the millions of people currently marching, protesting, and actively resisting the 2017 Trump presidency. "Vive la resistance!"

1. Mary Mahon, *US Health System Ranks Last Among Eleven Countries on Measures of Access, Equity, Quality, Efficiency, and Healthy Lives*, THE COMMONWEALTH FUND (June 16, 2014), http://www.commonwealthfund.org/publications/press-releases/2014/jun/us-health-system-ranks-last (Other countries included Australia, Canada, France, Germany, the Netherlands, New Zealand, Norway, Sweden, Switzerland, and the United Kingdom.).

2. *Id.*

3. *Id.*

4. *See About ONC*, HEALTHIT.GOV, https://www.healthit.gov/newsroom/about-onc (last updated May 12, 2016) (The U.S. government agency charged with coordinating public and private sector efforts to develop a nationwide health information technology infrastructure that support better health and better care at a lower cost.).

5. *See generally What is a Learning Health System,* LEARNING HEALTH COMMUNITY, http://www.learninghealth.org/ (last visited Oct. 22, 2017).

6. *Interoperability: A Shared Nationwide Interoperability Roadmap version 1.0,*

The impact these new technologies could have on our healthcare system would be profound, and they may not be too far away from becoming a reality.

This paper explains blockchain technology and analyzes how its incorporation into our health data infrastructure has the potential to create a more efficient national healthcare system, i.e. a learning health system (LHS). Second, this paper parses out the current paradigms that need to be changed in order for successful blockchain implementation to take place. Further, it discusses the contractual, legal significance of protocols embedded within a blockchain; and finally, it analyzes how these new technologies interact with the federal regulation governing healthcare data privacy, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[7]

The data in a patient's electronic health record comes from a variety of different sources. This "melting pot" characteristic has resulted in significant barriers to the evolution of our healthcare data infrastructure. To achieve the goal of a LHS, as set out by the ONC, these barriers must be overcome. The main barriers that should be addressed include: the fragmented nature of data, the heterogeneous nature of data, the timeliness of data,[8] and the current ownership and control paradigms as related to data. In addition, improvements are needed among healthcare entities for how they protect patients' data and the means by which patients gain transparency into the dissemination of their personal health information under healthcare privacy laws.[9] Blockchain technology can potentially address these issues and more.

Blockchain technology is actively used in the financial sector via cryptocurrencies, such as Bitcoin.[10] A blockchain is a distributed, tamperproof database that secures all records added to it. Each record contains a timestamp and a secure link to the previous record. This functionality enables users to potentially replace "certain inefficient, intermediary functions in different economic, social, and technological systems with decentralized digital networks."[11] This technology will be key in removing barriers and moving toward a LHS.

HEALTHIT.GOV, https://www.healthit.gov/policy-researchers-implementers/interoperability (last updated Dec. 22, 2015).

7. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPPA].

8. *See* CLAUDIA GROSSMANN ET AL., CLINICAL DATA AS THE BASIC STAPLE OF HEALTH LEARNING: CREATING AND PROTECTING A PUBLIC GOOD: WORKSHOP SUMMARY 77-78 (Institute of Medicine ed., 2010), https://www.ncbi.nlm.nih.gov/books/NBK54296/.

9. *See generally* C. Brodersen et al., *Blockchain: Securing a New Health Interoperability Experience*, HEALTHIT.GOV (Aug. 2016), https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf.

10. *See* Tal Yellin, Dominic Aratari, and Jose Pagliery, *What is Bitcoin?*, CNNMONEY, http://money.cnn.com/infographic/technology/what-is-bitcoin/ (last visited Oct. 22, 2017) (Bitcoin is a cryptocurrency created in 2009, where transactions are made without banks or transaction fees.).

11. Brodersen et al., *supra* note 9, at 3.

Aside from hindering technological issues, complications within the legal landscape also exist, specifically whether the self-executing protocols used within blockchain technology are legally enforceable, and whether the language of HIPAA needs to be expanded.[12] As of now, HIPAA applies only to traditional players in the healthcare industry or "covered entities."[13] HIPAA's protections do not extend to modern methods of collection, also known as non-covered entities (NCEs).[14] As the electronic sharing and storing of individual data increases and becomes more automated, organizations that are not regulated by HIPAA may collect, share or use individuals' health information, putting such data at risk of being misused.[15]

I. ONLINE IDENTITIES AND THE CURRENT HEALTH IT INFRASTRUCTURE

The evolution of online identities results from individuals' attempts to satisfy three basic principles: security, control, and portability.[16] Christopher Allen's article, *The Path to Self-Sovereign Identity,* describes the advancement of individuals' online identities in four stages: centralized, federated, user-centric, and self-sovereign.[17] The majority of individuals' online identities are centralized, meaning that they are "owned and controlled by a single entity, such as an e-commerce website or a social network."[18] There are numerous reasons that this format is inefficient. One reason is that this "siloed" nature leaves individuals' data vulnerable to cybersecurity attacks[19] and leaves users at the mercy of whichever online entity they have used since users do not own their online data.[20] The following language is often written into websites' Terms and Conditions: [website] "may, without telling you, immediately cancel or limit your access to your [website] accounts, certain [website] Services and any associated email addresses. . . ."[21] An individual's Internet identity can take years to create, holding

12. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

13. 45 C.F.R. § 160.103 (2014).

14. Examples of NCEs include mhealth technology (tablets, smartphones, applications, and wearable sensors or "wearables") and social media platforms.

15. *See generally* U.S. DEP'T OF HEALTH AND HUMAN SERV., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 2-7 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

16. Andrew Tobin & Drummond Reed, *The Inevitable Rise of Self-Sovereign Identity*, SOVRIN FOUNDATION 6 (Mar. 28, 2017), https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

17. Christopher Allen, *The Path to Self-Sovereign Identity*, LIFE WITH ALACRITY BLOG (Apr. 25, 2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

18. Tobin & Reed, *supra* note 16.

19. U.S. DEP'T OF HEALTH AND HUMAN SERV., *supra* note 15, at 4.

20. Tobin & Reed, *supra* note 16.

21. *Yahoo Terms of Service*, YAHOO!, https://policies.yahoo.com/ie/en/yahoo/terms/utos/index.htm (last visited Oct. 22, 2017).

significant value to its owner. Sometimes online identities are impossible to replace, yet the removal or deletion of an online account can erase a person's online identity.

The next step in this evolution, federation, gives portability to an individual's centralized identity.[22] At its most basic level, federation enables a user to log into "one service using the credentials of another. At a more complex level, it can allow different services to share details about the user."[23] A common example is online services and applications allowing a user to create an account using their Facebook or Gmail login. Federation provides limited portability and the power remains in the hands of the individual. The consequences of a federated account being removed or compromised is much more severe if that account is the user's key to other third party services.[24]

The third stage, a user-centric system, puts the "user in control of their own data, the accumulation of that data, and its release to third parties."[25] The core requirement for user control is that the information and data flow happens at the request of the user.[26] A user-centric system requires a user to select "an individual identity provider and agreeing to their often one-sided adhesion contracts. Because they are profit-driven businesses, the user becomes a product to be bought and sold, compromising independence and restricting true portability."[27]

Self-sovereign identity is the final step in Allen's article.[28] It provides all three necessary elements: individual control, security, and portability and "removes centralized, external control aspects from the three previous phases above."[29] The individual that the identity belongs to owns, controls, and manages his or her identity online; "a digital record or container of identity transactions that you control."[30]

The current healthcare data information technology infrastructure forms in the first three stages of the evolution discussed above. Typically, information will be "siloed" within a specific entity's server to which the patient will be provided a username and a password, but a user's rights are limited. While HIPAA and other regulations protect users, their scope is limited. HIPAA only applies to organizations known as "covered entities" and their "business associates:"[31] Based

22. Andrew Tobin & Drummond Reed, *The Inevitable Rise of Self-Sovereign Identity*, SOVRIN FOUNDATION 7 (Mar. 28, 2017), https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

23. *Id.*

24. *Id.*

25. *Id.* at 8.

26. *Id.*

27. *Id.*

28. Allen, *supra* note 17.

29. Tobin & Reed, *supra* note 22, at 8

30. Tobin & Reed, *supra* note 22, at 8.

31. U.S. DEP'T OF HEALTH AND HUMAN SERV., *supra* note 15, at 13-14. ("There are three types of covered entities: [1] health plans include health, dental, vision, health maintenance organizations (HMOs), Medicare, Medicaid, and long-term care insurers...employer-sponsored

on this definition, the evolution of the Internet and this type of data has resulted in legal gray areas. Ultimately, if a covered entity "hires an organization to offer a [personal health record] in the covered entity's name and to host the health information collected in that [personal health record] for the covered entity, that [personal health record] vendor is acting as the covered entity's business associate."[32] The next sections discuss the ways in which the heath care sector has exploded with new types of data and methods of data collection. Along with these changes, the third parties handling personal health data have changed with many falling outside the scope of the established definition given to their predecessors. By allowing these new organizations to manage personal health data without proper regulation, security measures are weakened and individuals' sensitive information are at risk.

II. BLOCKCHAIN TECHNOLOGY

It is helpful to have a basic understanding of what a blockchain is and how it works before discussing how this technology can affect the privacy of healthcare data and potentially increase efficiency. A blockchain is a cryptographic protocol[33] that allows a "network of computers (nodes) collectively to maintain a shared ledger of information without the need for complete trust between the nodes."[34] An easy way to think of a shared ledger is in the context of earthquakes. In a region, there are multiple seismographs monitoring earthquake activity. As an earthquake occurs, each regional seismograph records an identical reading of that earthquake.

Along the same vein, each blockchain is essentially a time-sequenced chain of events (in this context, transactions within the healthcare industry) that have been authenticated using a consensus mechanism, specified by the protocol.[35] The consensus mechanism guarantees that if the majority of the nodes in the network validate the transactions posted to the ledger per the stated governance rules,[36]

---

group health plans, government and church-sponsored health plans, and multi-employer health plans; [2] health care clearinghouses; and...[3] health care providers who electronically conduct certain transactions, such as claims submissions and prior authorizations....[A] business associate is a person or organization that uses PHI to perform covered functions or activities on behalf of a covered entity.").

32. U.S. DEP'T OF HEALTH AND HUMAN SERV., *supra* note 15, at 14.

33. Chris Kemmerer, *What is a "Cryptographic Protocol?"*, SSL.COM (Mar. 10, 2015), https://www.ssl.com/faqs/what-is-a-cryptographic-protocol/ ("A protocol is simply a set of rules or instructions that determine how to act or interact in a given situation. A cryptographic protocol is designed to allow a secure communication under a given set of circumstances.").

34. Brodersen et al., *supra* note 9.

35. Hans Lombardo, *KPMG Report on Blockchain Consensus Mechanisms*, CHAIN-FINANCE.COM (Jul. 8, 2016, 10:00 AM) http://blockchain-finance.com/2016/07/08/kpmg-report-on-blockchain-consensus-mechanisms/ ("[A] consensus mechanism is the way in which a majority (or in some mechanisms, all) network members agree on the value of a piece of data or a proposed transaction, which then updates the ledger.").

36. Josh Stark, *Making Sense of Blockchain Governance Applications*, COINDESK (Nov. 20,

information stored on the blockchain can be trusted as reliable.[37] This process ensures that the transaction data is replicated consistently across the network (like the seismograph example). The effect of the distributed consensus mechanism typically requires that every node within the network contain the entirety of information stored on the blockchain.[38]

A. EFFICIENCY AND TRUST IMPROVEMENTS

Many of the major barriers to efficient healthcare are related to data usage. The wide distribution of data across systems and significant fragmentation make it hard for healthcare providers to use data efficiently.[39] Data is collected and stored in many places—patient records, provider(s) and government repositories—for public health and planning purposes. However, few places have comprehensive and longitudinal views about the individuals in their systems.[40] The inability to connect data, which could include risk factors, medical history, and interventions, in a comprehensive way is a serious flaw in progressing forward.[41]

Besides the fragmentation of data, the data itself is heterogeneous. Some data, such as diagnosis, procedure, medication, laboratory and administrative data, are "usually of high quality, coded and computerized."[42] However, most other data is unavailable in computerized form, or it is in free form (doctor's notes), even if it is computerized.[43] Timeliness of data is also a concern because of the wide range of availability in different data. Clinical data is almost always immediately available; administrative data that has been coded may take days or weeks to become available; and statistics in government repositories may lag by two or more years.[44]

Blockchain technology could eliminate these barriers by providing a peer-to-peer repository containing all of this data, thus reducing fragmentation. Protocols within the chain can ensure that data is uniformly coded and consistent throughout the system, creating a homogeneous environment conducive to fluid exchange. Finally, this data can be loaded instantly into the blockchain, and be provided to anyone with an access key via the distributed ledger functionality.

2016), http://www.coindesk.com/making-sense-blockchain-governance-applications/ ("[T]he processes and systems used to facilitate decision-making in any organization.").

37. Brodersen et al., *supra* note 9, at 5.

38. Brodersen et al., *supra* note 9, at 5.

39. *See* CLAUDIA GROSSMANN ET AL., CLINICAL DATA AS THE BASIC STAPLE OF HEALTH LEARNING: CREATING AND PROTECTING A PUBLIC GOOD: WORKSHOP SUMMARY 77-78 (Institute of Medicine ed., 2010), https://www.ncbi.nlm.nih.gov/books/NBK54296/.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

Similar to financial transactions, trust is imperative to data within the healthcare industry. Health information is controlled by hospitals; health information exchanges; insurance companies; and other intermediaries, who, while claiming trustworthiness, are in a position to exploit that trust. Blockchain technology reduces the role of these trusted intermediaries in securing and sharing individuals' health records, thus shifting the power balance in favor of doctors and patients.[45]

However, blockchain technology cannot solve all of the trust concerns surrounding health data protection. The United States should follow the European Union and enact stronger regulations, which, coupled with blockchain technology, would affirm a paradigm shift in data ownership. The new European Union model casts a wide net and identifies personal data as "any information related to an individual, whether it relates to their private, professional, or public life."[46] The objective of the General Data Protection Regulation (GDPR), is to give individuals ownership over their data.[47] Ownership is accomplished by imposing strict sanctions for misuse, making "automated individual decision making" contestable, requiring explicit consent for the collection and use of data, and giving individuals a clear right of erasure.[48]

The United States should take these rules one step further. In enacting new data privacy legislation, an additional right of control should be included to fully vest the individual. Patients should be able to source their own health information and data when it is practical to do so. However, then a second paradigm, medical liability, must also be addressed. The threats of medical malpractice lawsuits or HIPAA violations already create a distrust in handling health information sourced by an individual. When a provider is administering care to a patient, it is imperative that the health record is accurate, so the patient receives the best possible care. The consequences of this information being inaccurate are potentially deadly. Blockchain technology can assist in certain situations by lending creditability and accuracy to a digitally signed copy of patient-sourced health information.[49] This process would help alleviate fear on the provider's side, regarding data trustworthiness, and allow a provider to more easily incorporate said data into the decision-making process when caring for a patient.

---

45. Adrian Gropper, *Blockchains Power the Physician-Patient Relationship*, SOC'Y FOR PARTICIPATORY MED. (Oct. 10, 2016), http://participatorymedicine.org/2016/blockchains-power-the-physician-patient-relationship/.

46. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L. 119) 1.

47. *See id.*

48. *Id.*

49. *See generally* Brodersen et al., *supra* note 9, at 5.

A blockchain has pre-written and coded protocols, also known as smart contracts, that determine how to act or interact depending on a situation.[50] Once an individual provides a receiver (doctor or healthcare entity) with a cryptographic key, the receiver has the necessary authorization for the specific transaction and then the distributed ledger verification system ensures that both parties are trustworthy and that any information exchanged is reliable.

These features can also immensely improve the auditability of each transaction since the system creates a time-stamped link from the most recent transaction to the previous transaction, i.e., the chain.[51] Further, to ensure the integrity of the data, governance rules of a blockchain solution would pre-define access and control permissions.[52]

B. LEGALLY ENFORCEABLE SMART CONTRACTS

The term "smart contract" tends to be overloaded. Many people assume that these protocols will automatically be legally enforceable. However, whether this is so in a given situation, may turn in part on the type of smart contract at issue, the factual matrix within which it operates, and the applicable law determining the issue.[53] Foundational regulatory frameworks have already been established, both domestically and internationally, such as "E-SIGN,"[54] the Uniform Electronic Transactions Act (UETA),[55] and the United Nations Commission on International Trade Law's Model Law on Electronic Signatures (MLES),[56] thus the electronic nature of a smart contract is unlikely to be problematic.

However, beyond these base frameworks, questions remain as to how the above listed legal requirements are best reflected in code, if at all. At this point in time, it appears that these protocols cannot handle all of the intricacies that must be included in real-world, natural language contracts. The easiest way to incorporate intricacies is through dual-integration. Dual-integration takes a smart contract and links it to a corresponding version of a fully-integrated, natural language contract. By linking the protocol to an actual paper contract, it allows parties to limit their exposure to risk by including very detailed, contractual language. All of this language cannot efficiently

---

50. *See generally Smart contract*, WIKIPEDIA, https://en.wikipedia.org/wiki/Smart_contract (last updated Oct. 27, 2017).

51. Brodersen et al., *supra* note 9, at 2-3.

52. Brodersen et al., *supra* note 9, at 3.

53. *Can smart contracts be legally binding contracts?*, R3 & NORTON ROSE FULBRIGHT, LLP 4 (Nov. 2016), http://www.nortonrosefulbright.com/files/norton-rose-fulbright--r3-smart-contracts-white-paper-key-findings-nov-2016-144554.pdf.

54. 15 U.S.C. § 7001 (2000).

55. CAL. CIV. CODE § 1633.1 (West 2000).

56. *See UNCITRAL Model Law on Electronic Signatures (2001)*, UNCITRAL.ORG, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html (last visited Oct. 30, 2017).

be included in the computer code, that is a smart contract, but without it, it is unlikely smart contracts can be legally enforceable. In addition, having the paper contract contain the code, allows parties to present tangible evidence to a judge or arbitrator if a dispute arose.

For a court handling a smart contract dispute, deciding which legal jurisdiction controls or which country's law governs could be difficult. Courts are accustomed, however, to dealing with difficult jurisdictional issues relating to contracts being formed over the Internet. Jurisdictional problems in the case of smart contracts can be avoided by the inclusion of the appropriate choice of law and jurisdiction clauses incorporated into the code by reference to the corresponding paper contract. However, recovery, or enforcement of judgments or resolutions, could still prove problematic when dealing with exchanges between the borders of various countries.

Another issue is that natural language contracts often result in complex arrangements between parties. A sophisticated legal contract usually contains a number of legal phrases that are not well suited for coding and may only be determined by legal analysis, applying principles of contractual interpretation, which is usually determined by a judge.[57] Phrases such as: "material adverse change," "reasonable endeavors," or "reasonable notice" all are questions of degree, whose formulation involves judgment.[58] As technology improves, smart contracts will likely be constructed in a legally enforceable manner. However, for the foreseeable future, smart contracts must be connected to a natural language contract, leaving a role for both lawyers and judges in the development of this space.

C. SOVRIN'S ONLINE IDENTITY SYSTEM

Organizations are already investing many resources into blockchain technology to tackle today's hardest questions surrounding health data. One such organization, Sovrin, has developed a way to use this technology to create an online identity system:

> An internet-like identity system would allow any person, organisation, or thing to have an identity relationship (something we call a "claim" in the world of identity) with any other. And to do this without the need for authorisation from someone else. Because anyone can use these identities and the resulting relationships without an intervening authority, they're called "self-sovereign."[59]

Sovrin views the self-sovereign identity as the final step in the evolution

57. *See Smart Contracts: coding the fine print*, NORTON ROSE FULBRIGHT, LLP 12 (Mar. 2016), http://www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print.

58. *Id.*

59. Andrew Tobin & Drummond Reed, *The Inevitable Rise of Self-Sovereign Identity*, SOVRIN FOUNDATION 1 (Mar. 28, 2017), https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

of Internet identity.[60] This "evolution of the Internet will be the creation of a common identity layer that allows people, organisations and things to have their own self-sovereign identity—a digital identity they own and control, and which cannot be taken away from them."[61]

The impact of this missing layer is becoming more evident as more individuals depend on digital services in their daily lives.[62] Without an identity layer, health information is "siloed" into individual databases – a naïve attempt to safeguard hundreds of different user passwords. The person or organization to which "the identity pertains owns, controls, and manages" that identity; no one can take one's self-sovereign identity.[63]

This proposed identity layer is easy to think of as a digital record or container of identity transactions that the individual controls.[64] One can add more data or ask others to do so. One can give consent to share data with others, and easily facilitate that sharing.[65] This self-sovereign identity has been described as an "Internet for identity," which much like the actual Internet, has three important virtues: no one owns it, everyone can use it, and anyone can improve it.[66]

Sovrin created a hybrid distributed ledger model that delivers public access with trusted governance.[67] The Sovrin identity network comprises multiple, distributed nodes located around the world.[68] Nodes are hosted and administered by stewards, who validate identity transactions to assure consistency, and each node has a copy of the ledger.[69] It is believed that this type of system could enable rich innovation through the open source nature of its code.[70]

---

60. *Id.* at 8.

61. *Id.* at 3.

62. *See id.* at 4; *see also Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels*, PR NEWSWIRE (May 27, 2015, 6:00 PM), http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html; *see also The Threat of Fake Users,* TELESIGN.COM, https://www.telesign.com/fake-user-impact-report/ (last visited Oct. 30, 2017).

63. Tobin & Reed, *supra* note 59, at 8.

64. *See* Tobin & Reed, *supra* note 59, at 8.

65. *See* Phillip J. Windley, *How Sovrin Works: A Technical Guide from the Sovrin Foundation*, SOVRIN FOUNDATION 7 (Oct. 3, 2016), https://sovrin.org/wp-content/uploads/2017/04/How-Sovrin-Works.pdf.

66. Phil Windley, *An Internet for Identity,* PHIL WINDLEY'S TECHNOMETRIA (Aug. 29, 2016, 2:30 PM), http://www.windley.com/archives/2016/08/an_internet_for_identity.shtml.

67. Report by the UK Government Chief Scientific Advisor, *Distributed Ledger Technology: beyond block chain* (Gov't Off. for Sci., 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (defining a distributed ledger as a "database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds.").

68. *See Sovrin Glossary: A glossary of terms used in Sovrin documentation,* SOVRIN FOUNDATION 3 (Sept. 29, 2016), https://sovrin.org/wp-content/uploads/2017/04/Sovrin-Glossary.pdf.

69. *Id.*

70. Tobin & Reed, *supra* note 59, at 12.

As good as all of this may sound, many remain skeptical. For this type of fundamental shift to be successful, it must first be accepted. Are those currently holding power as "trusted institutions" going to be willing to give up that power? Many of these entities make a considerable amount of money being identity providers, and giving up that power would be counterproductive to their interests.

III. THE CURRENT FEDERAL LANDSCAPE

As the Internet evolves, the way people access it does too, whether it be a new mobile application, or a new version of Fitbit[71] to track daily exercise routines or how many calories burned. As blockchain technology is improved and implemented into these systems, many of the ways in which data is collected, stored, and transferred will begin to fall outside the scope of HIPAA.[72] To address this foreseeable problem, the language in HIPAA must be updated, or such as the case within the European Union, the United States must commit resources towards the development of new data privacy regulations[73] that treat all data, as objects worthy of stringent privacy and use protections.

Since implementing HIPAA twenty-one years ago (21),[74] the landscape of health data has gone through a dramatic evolution as new technologies have become available. This change has left significant portions of individuals' electronic health records vulnerable to misuse.

Non-covered entities take many forms; however, the two most prevalent in society are mHealth technologies and social media applications.[75] These technologies give individuals the ability to become more engaged and aware of their health, and they serve as an alternative means of collecting and exchanging health information."[76] However, these technologies and applications could present privacy issues, as they are outside of HIPAA's protections, allowing third parties to share data with multiple other parties.[77] Social media applications encourage sharing information, preferences, and views among individuals and groups, and allow self-disclosure of health information. These websites are frequently used by patients to discuss treatment options and provide support networks. Twenty-seven

71. FITBIT, https://www.fitbit.com/home (last visited Nov. 4, 2017).

72. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

73. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L. 119) 1.

74. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

75. *See generally* U.S. DEP'T OF HEALTH AND HUMAN SERV., *supra* note 15, at 1 (mHealth technologies include tablets, smartphones, software applications and wearable sensors such as Fitbit, Apple Watch, etc.).

76. U.S. DEP'T OF HEALTH AND HUMAN SERV., *supra* note 15, at 8. ("mHealth technology allows individuals to monitor daily activities and record vital signs or other biometric data outside of equipment in their doctor's office.")

77. U.S. DEP'T OF HEALTH AND HUMAN SERV., *supra* note 15, at 8.

percent (27%) of Internet users and twenty percent (20%) of adults have tracked their weight, diet, exercise routine, symptoms, or other health indicators, online.[78] Like mHealth technologies, social media websites also collect health data and often fall outside the protections of HIPAA, placing individuals' privacy and data at risk.

A. HIPAA'S SCOPE

HIPAA is enforced by the Office for Civil Rights.[79] Congress also granted "State Attorneys General the authority to enforce the HIPAA Rules and called on the U.S. Department of Justice to enforce violations of the criminal provisions of HIPAA."[80] HIPAA applies to a wide range of organizations, "but a growing number of organizations that maintain, transmit, or receive health information" continue to fall outside its scope.[81] The Act has three main parts: the HIPAA Privacy Rule,[82] the HIPAA Security Rule,[83] and the HIPAA Breach Notification Rule.[84] The HIPAA Privacy Rule protects the privacy of protected health information (PHI) in the hands of covered entities and business associates.[85] The HIPAA Security Rule sets national standards for the security of electronic PHI.[86]

1. The HIPAA Privacy Rule

The HIPAA Privacy Rule provides "federal protections for individually identifiable health information held by covered entities and their business associates and gives patients" a plethora of rights regarding that information.[87] Typically, a covered entity may still legally use and disclose personal health information without formal authorization for many purposes.[88]

Covered entities can rely on professional ethics and their best

78. Susannah Fox, *The Social Life of Health Information, 2011*, PEW RESEARCH CENTER 3 (May 12, 2011), http://www.pewinternet.org/~/media/Files/Reports/2011/PIP_Social_Life_of_Health_Info.pdf.

79. OFFICE FOR CIVIL RIGHTS, https://www.hhs.gov/ocr/index.html.

80. U.S. DEP'T OF HEALTH AND HUMAN SERV., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 13 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

81. *Id.*

82. 45 C.F.R. § 164.514(e) (2013).

83. 45 C.F.R. § 164.306 (2013).

84. 45 C.F.R. § 164.404 (2013).

85. U.S. DEP'T OF HEALTH AND HUMAN SERV., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 13 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

86. *Id.*

87. *Id.* at 14.

88. *Id.* at 15 (including "for treatment, payment, and health care operations ...; directly to family, friends, and others involved in the individual's care unless the individual objects; for certain specified activities beneficial to the public...; where expressly required by law; and as a Limited Data Set for the purposes of research, public health, or health care operations").

judgment when deciding whether to use or disclose personal health information as permitted by HIPAA. However, they must obtain written authorization from individuals to use or disclose their information for reasons not permitted by HIPAA.[89]

HIPAA Privacy Rule protections do not extend to data held by non-covered entities or to individual health information that has been de-identified.[90] Because of this provision and non-covered entities not being subject to de-identification standards, there is little understanding of how non-covered entities sharing de-identified information impacts individuals' privacy and whether the standards used by non-covered entities to de-identify information meets the standards as outlined by HIPAA.[91]

2. The HIPAA Security Rule

The HIPAA Security Rule requires covered entities and business associates to perform a security risk assessment to identify and mitigate risks to the confidentiality, integrity, and availability of the electronic PHI they create, receive, maintain, or transmit.[92] The rule specifies "administrative, physical, and technical safeguards that covered entities and their business associates must implement to prevent unauthorized or inappropriate access, use, or disclosure" of electronic PHI.[93] The administrative safeguards required include risk analysis and management, access management, workforce training, and the evaluation of security measures.[94] The physical safeguards required are physical measures, policies, and procedures to safeguard the covered entity or business associate's electronic information systems.[95] The "technical safeguards include access controls, audit controls, integrity, person or entity authentication, and transmission security."[96]

B. ANALYSIS OF CURRENT REGULATIONS

As healthcare data systems have evolved, regulations have lagged

89. *See Health Information Privacy: Research*, U.S. DEP'T OF HEALTH AND HUMAN SERV., http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html (last updated Jun. 16, 2017).

90. 45 C.F.R. § 164.502(d) (2013); *see also* 45 C.F.R. § 164.514(b) (2013) (There are two methods of de-identification: the use of statistical methods proven to render information not individually identifiable; and the deletion of eighteen specified identifiers.).

91. U.S. DEP'T OF HEALTH AND HUMAN SERV., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 4 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

92. 45 C.F.R. § 164.306 (2013).

93. U.S. DEP'T OF HEALTH AND HUMAN SERV., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 16 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

94. *Id.*

95. *Id.*

96. *Id.*

behind. This lag affects how companies are regulated and how they handle individuals' personal health data and information. Looking at the legal landscape there appear to be several ways in which HIPAA's protections fail to apply in the context of non-covered entities. Three main areas of concern are individuals' access rights, third parties' re-use of data, and security standards applicable to data holders and users.[97]

One of the most important ways that non-covered entities differ from HIPAA-protected entities pertains to the right of individuals to access their PHI held by an organization.[98] The rights laid out under HIPAA, including the access to PHI, the ability to demand an accounting of "disclosures, and some control over how the information is used and shared, do not exist for information held by" non-covered entities.[99] The current practices of non-covered entities often lack transparency, as they are not required to provide individuals with access to data about themselves. Although a non-covered entity may make "representations to consumers about access, these are not required by law[;]. . . an individual may share data about his or her health through mHealth technologies or health social media but may not" be able to later obtain a copy of the "information or learn where the data was re-disclosed."[100]

The HIPAA Rules dictate to whom and for what purpose a covered entity may disclose PHI. However, once released, the protections of HIPAA may not apply. In that sense, HIPAA's defined list of permissible disclosures helps limit third parties' access and use of sensitive health information. One particularly important limitation "is in the use of health information for marketing."[101] Individuals who provide their data to non-covered entities likely will not enjoy the same protections or have recourse.

The first step that must be taken, from a regulatory perspective, is to expand HIPAA. This step would be an easy, temporary solution, while more extensive legislation is developed. The most efficient change would be to simply broaden the language defining covered entities in HIPAA to include current mHealth technologies and social media websites. However, this language should be left somewhat broad to allow for the incorporation of future, unanticipated technologies and devices. This change would help address some of the gaps in current regulations.

The second step, arguably the most important, is the fruition of a blockchain database for national healthcare data. Implementing such a database could make HIPAA's Privacy Rules and individual access

97. *Id.* at 20.
98. *See id.*
99. *Id.*
100. *Id.* at 21.
101. *Id.* at 22.

rights obsolete if it could successfully re-distribute the ownership of health data back to the individual. HIPAA would still be necessary to control what happens to this data after it has been released by an individual and flows downstream, as well as in scenarios of data breach and any required notification thereafter.

CONCLUSION

In a perfect world one could envision such a database allowing an individual instant access to his or her health information on a smartphone. Then one could view, share, and delete any and all data from a mobile device. As of November 21, 2016 this ideal world has come a few steps closer to becoming a reality. The Bill and Melinda Gates Foundation[102] awarded the technology company, Factom,[103] a large grant for deploying blockchain technology for medical records.[104] The company will use the grant to focus on secure access of health data via smartphones in developing nations. Individual medical records secured by Factom's blockchain addresses ensure uptime and access, despite the challenges of geopolitical instability and the population relocations it can cause.[105] Peter Kirby, CEO and Co-Founder of Factom, told Bitcoin Magazine that blockchain's distributed data characteristics are well suited to maintaining the privacy and security of medical records, even in environments with low rates of web connectivity.[106]

With blockchain technology trust negotiations in the healthcare industry would be seamless and inexpensive. Researchers would have access to de-identified data to find cures for what ails society, and doctors could see each patients' health in a longitudinal view, providing more accurate diagnosis and avoiding unnecessary, duplicative procedures. Individuals would also always know how and where their data was being used because they either authorized the use or could trace the path of their data with the enhanced auditability features of blockchain technology. So there you have it, the "future" is already upon us.

---

102. BILL & MELINDA GATES FOUNDATION, https://www.gatesfoundation.org/.

103. FACTOM, https://www.factom.com/.

104. Mike Miliard, *Gates Foundation gives Factom a grant to deploy blockchain for medical records*, HEALTHCARE IT NEWS (Nov. 21, 2016, 12:36 PM), http://www.healthcareitnews.com/news/gates-foundation-gives-factom-grant-deploy-blockchain-medical-records.

105. *Id.*

106. *Id.*