Unleash the Data: Blockchain Technology and the Potential for Its Use in Health IT

Kristen F. Johns
Kristen.Johns@wallerlaw.com

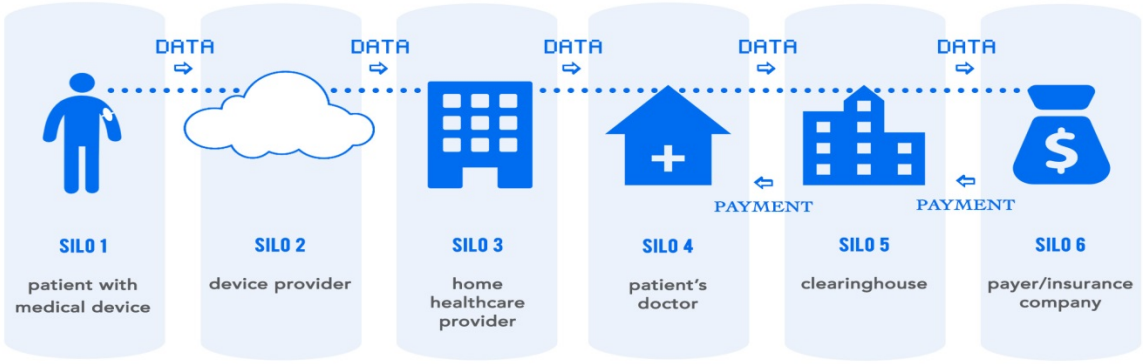
Blockchain technology has the potential to shift control of data to the patient and to unleash information currently held in centralized systems to all entities involved in providing healthcare services. Unleashing data will result in fundamental shifts in the way healthcare is provided to not only individual patients but also the general U.S. population.

1. Introduction

While the conversations surrounding blockchain technology understandably focus on the benefits of the technology, the underlying infrastructure used in the blockchain could fundamentally reshape the landscape of healthcare and the ways in which care is delivered by providers and received by their patients. Proponents of blockchain technology understandably focus on benefits, such as data quality, process integrity, and transparency. Within the healthcare context, however, blockchain technology could fundamentally reshape how healthcare information is delivered and managed. The current landscape comprises disparate entities that work together to deliver care to a patient. Commentary to date has focused at a high level on the promise of blockchain technology, but the analysis requires a deeper dive into how and where data flows, and this begins by identifying the entities that currently have access to it. Blockchain technology has the potential to shift control of healthcare information to the patient and, in the process, to unleash information currently held in centralized networks to new entities, all of which are currently a part of delivering healthcare services.

2. Problem: Health Information Is Segregated

Our current healthcare system comprises a seemingly countless number of disparate entities with respect to patient care. Only the ardent privacy advocates appreciate the extent to which data is collected, accessed, and used once a person enters the healthcare system. For example, if a patient wears a blood pressure monitoring device, every entity that enables the device to function might participate in the information flow as the device receives patient data and relays that data downstream. This might include the medical device manufacturer, the healthcare provider (e.g., a hospital or doctor's office), and an intermediary (e.g., home health care provider). The American Recovery and Reinvestment Act of 2009 (ARRA) for certified professionals requires that patients have access to their information, but the information is siloed in disparate systems with no central reference. (This requirement does not apply to certain entities such as home health providers or device manufacturers.) Therefore, while a large portion of the data has become digitized as part of this Act, it is still not easily shared across all entities in the healthcare system.



Complicating this scenario, each entity typically asserts a right in the data to which it has access. In the United States, the use of this data is governed by the Health Insurance Portability and Accountability Act (HIPAA), where the parties contracting for services are placed into roles of either a Covered Entity or a Business Associate.[1] In the current market, data reigns supreme, however, and this "land grab" for data as well as the associated restrictions on use of data have had numerous (probably unintended) results.

Efforts have been made by various entities to disclose and share patient health information and are well-known. CMS continues to expand its release of Medicare data under the Medicare Access and CHIP Reauthorization Act (MACRA),[2] most recently requiring qualified entities to combine Medicare data with other claims data to generate reports and supplier performance metrics across multiple payers. Although Health Information Exchanges (HIEs) strive to be a sustainable, trustworthy source of data, they have come under scrutiny for their ability to promote interoperability goals, including restrictions on data.[3] In addition, HIEs typically shift the risk of potential liability to the respective entities that comprise the HIE.[4] Finally, Accountable Care Organizations impose similarly strict protections on data sharing for participating member. Ultimately, although certain parties benefit from these entities, none of these fractured systems of sharing and using data offer long-term solutions because only certain portions of data are accessible to a select few.

The aforementioned assertions of data ownership hinder the goals of the Interoperability Roadmap and other regulatory endeavors because each entity stakes a claim to data, and in some cases, uses it as leverage in contract negotiations or is unwilling to share. Instead, these entities prize the data and protect it for data analysis purposes. Pending legislation introduced by Senator Lamar Alexander in the Improving Health Information Technology Act[5] addresses specific issues with respect to data, and highlights industry and regulatory concerns by introducing an amendment, which includes a Section titled, "Empowering Patients and Improving Patient Access to Their Electronic Health Information." The legislation adds the following definition:

> The term 'information blocking' means (A) with respect to a health information technology developer, exchange, or network, business, technical, or organizational practices that (i) except as required by law or specified by the Secretary, interferes with, prevents, or materially discourages access, exchange, or use of electronic health information; and (ii) the developer, exchange, or network

> knows, or should know, are likely to interfere with or prevent or materially discourage the access, exchange, or use of electronic health information; and (B) with respect to a health care provider, the person or entity knowingly and unreasonably restricts electronic health information exchange for patient care or other priorities as determined appropriate by the Secretary.

The Act goes on to define activities that both constitute and do not constitute information blocking. This mandate to encourage access, exchange, or use of electronic health information flies in the face of currently held policies of private, institutional entities throughout the healthcare system. Blockchain technology can solve this apparent conflict. Proponents of this sophisticated ledger system believe blockchain technology could eliminate the need for this statutory definition by removing the possibility any "information blocking."

3. Clearinghouses: Treasure Trove of Health Information

An often overlooked entity in the current healthcare system workflow is the Health Care Clearinghouse, which is defined by HIPAA as:[6]

> a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:
>
> 1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
> 2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Importantly, HIPAA defines Healthcare Information as:

> any information, including genetic information, whether oral or recorded in any form or medium, that:
>
> 1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
> 2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health information in an aggregated form drives the engines of ingenuity and desire in a manner improves care at all levels, from the individual patient to the general population. Of the entities listed in the statute, the clearinghouse has access to all health information.

Clearinghouses are statutorily and oftentimes contractually limited in their use of the vast amounts of information to which they have access. For example, a clearinghouse can be a Business Associate to Covered Entity customers that often do not relinquish their rights to data as a matter of enterprise-wide policy, unless such relinquishment would directly benefit the Covered Entity. These contractual restrictions supersede the permissions granted by HIPAA to de-identify and aggregate health information. HIPAA does permit Covered Entities, however, to use and disclose Protected Health Information (PHI), with certain limits and protections, for treatment, payment, and healthcare operations activities. This permission is granted to avoid interfering with an individual's access to quality health care or the efficient payment for such healthcare.[7] These three criteria establish the platform upon which all data analytics is based.

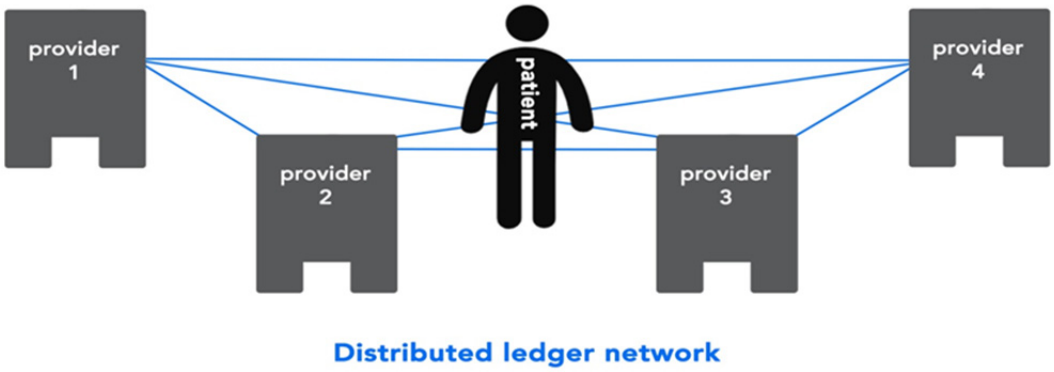
There are relatively few clearinghouses in the United States. The largest clearinghouse is Change Healthcare, which processed nearly nine billion transactions in 2015.[8] Access to the transactional data processed by clearinghouses could provide the longitudinal patient health record that innumerable entities and organizations are trying to achieve. Availity, Experian Health, and the SSI Group, Inc. have formed the Claim (Your Health Data) Coalition to "advance the availability of health data and records for patients and other stakeholders in the healthcare system."[9] Clearly, there is a need – and a desire on behalf of at least some of the primary stakeholders – for health information to be shared. Access to clearinghouse data, through legislative reform or through the implementation of blockchain technology, would revolutionize healthcare.

4. Prospective Use: Blockchain for Patient Identity

The most obvious and often-cited example of blockchain technology in the healthcare context is the creation of a longitudinal, secure a patient record on a per interaction, or encounter, basis.[10] In today's healthcare system, there are mechanisms in place to obtain patient permission for the right to share data in either paper or digital form. If a provider were incorporating blockchain technology into its information technology system, the provider would requests permission to access the patient's ledger, or appropriate portions of the ledger. The country of Estonia has already adopted Keyless Signature Infrastructure technology to secure patient records. Citizens of Estonia are part of a centralized, paperless system through the help of Guardtime, a private company integral in Estonia's implementation of blockchain technology.[11] Because several U.S.-based corporations are already investigating potential blockchain solutions, it is unlikely the same tactical approach will be implemented, but the general model exists and is in use. It has been shown that blockchain technology can be used to build a comprehensive patient health record, which is the Holy Grail of any electronic health record system.

If the United States were to incorporate blockchain technology into its healthcare infrastructure – even initially in a segregated population – all data would be gathered and secured in a prospective manner. As the blocks would be chained together, the record would grow stronger. While the prospective nature of this implementation, would not help individuals in their later years of life or individuals with extensive, significant medical histories, the addition of their data to the ledger would create a secure record, benefitting both the patient and any entity in the trusted ledger network. This would also shift some of the roles among healthcare entities, specifically Covered Entities and Business Associates.

Business Associates are beholden to Covered Entities because Business Associates act on behalf of a Covered Entity to perform certain functions, such as the creation, receipt, maintenance, or transmission of PHI.[12] Currently a patient can access his/her PHI upon specific request, but blockchain technology would remove the necessity for the request. Blockchain technology would shift all roles in relation to the underlying transactions, where no party would have leverage over the other regarding data sharing or transfer. Instead, the structure would transition from a "workflow" to a "(permissioned) distributed ledger" among all participants. The silos would disappear. This would create a fundamental shift in healthcare laws and the ways in which they are enforced. Blockchain technology would eliminate the leverage of a Covered Entity over a Business Associate with respect to data, since all parties are part of the same network, utilizing secure methodologies and algorithms to ensure the security of data in the blockchain. The "land grab" for data would be eliminated, with all parties having equal access to health information.



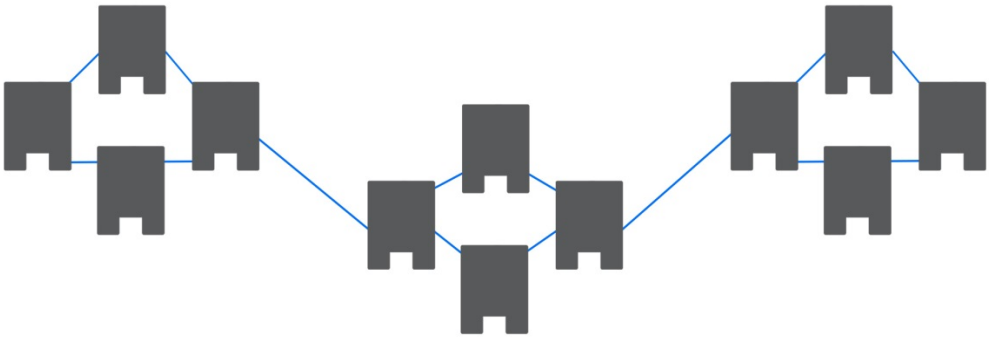
5. Retrospective Analysis: Strengthening the Value of a Patient Record

While a prospective record would be beneficial for a newborn, creating a comprehensive, or longitudinal, health record for all citizens using blockchain technology will require a retrospective collection and of analysis of applicable data. Considering the disparate entities that form our healthcare system, it may seem like an impossible task.

Clearinghouses may hold the key (or digital signature) to create a sensible, usable, and comprehensive electronic patient record. Inserting a node with patient data into the patient's permissioned ledger would provide the requisite information to make the effort to adopt blockchain technology meaningful and worthwhile. Entities could leverage the vast amounts of data in clearinghouses and payers. In fact, some estimate the incorporation of historical data into a ledger could occur within approximately five years.[13] This "data dump" would serve as a foundation to build a patient's record using blockchain technology. Such a feat would realize the numerous goals established by Office of the National Coordinator for Health Information Technology (ONC) and other applicable regulatory agencies by empowering individuals to truly have trusted and simplified access and security to their health information. In this model, the transactions recorded on the ledger include and are based on the exchange and use of Protected Health Information.

6. Retrospective Analysis: Leveraging Existing Data for Analytics

Blockchain technology could also be used in a way that is somewhat analogous to the publication of the human genome. The publication of the human genome allowed scientists worldwide to have access to previously unknown information. This information is currently access and mined on a daily basis to elucidate genomic patterns and generally further research in innumerable diseases. In a similar way, certain refined clearinghouse data (or other entities with access to large data sets) could be published on a peer-to-peer network architecture. Such networks are decentralized and open, similar to Bitcoin and Napster.[14] Thus, instead of a comprehensive patient record, data would be de-identified in compliance with HIPAA.[15] Such staggering amounts of data would be a treasure trove for any entity with proprietary algorithms and data analytics expertise. A node could be created based on this de-identified information and accessed on a decentralized network. As noted in recent breaches, however, decentralized networks are not without an element of risk. The consensus mechanism inherent in the decentralized network depends on having a majority of users behaving honestly. As Napster granted users the ability to access songs, this decentralized healthcare network with this type of information could provide access to entities seeking valuable, agnostic information. This information can be used to answer specific questions or goals in the provision of care, and access to the could inspire further innovation and meaningful growth to the healthcare system.



Decentralized ledger network

7. Conclusion

The largest EHR vendor in the United States is Epic Software. Epic's heavily guarded software is based on a programming language called MUMPS (Massachusetts General Hospital Utility Multi-Programming System). This language was developed in 1966. Fifty years later, it is time to incorporate the promise of cutting-edge technology into the healthcare system. Blockchain technology has the potential to revolutionize the creation of and access to comprehensive electronic health records as well as to unblock data that is currently held as a valuable asset. Opening access to information will empower individuals and allow providers and payers to use data to inform decision-making. The seamless flow of data on a blockchain ledger have the potential to reinvent the way health information is accessed and used. The type of ledger will depend on the underlying purpose and will rely on specific nodes and supporting functionality. Blockchain technology offers a cryptographically secure technology with diverse applications,

and has the potential to initiate a revolution that could materially alter healthcare for the mutual benefit of individuals and all the entities that comprise the healthcare network in the United States.

References

[1] *See* Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936 (1996).
[2] *See* 42 C.F.R. § 401 (2013).
[3] J.R. Vest and L.D. Gamm, "Health information exchange: persistent challenges and new strategies," *J. Am. Med. Inform. Assoc.* 17:288-94 (2010).
[4] K. Lee, "Data blocking: When health information exchanges don't live up to their name," http://searchhealthit.techtarget.com/opinion/Data-blocking-When-health-information-exchanges-dont-live-up-to-their-name and the Office of the National Coordinator for Health Information Technology Report to Congress: Report on Health Information Blocking (April 2015).
[5] S.2511, 114th Cong. § 7 (2016).
[6] *See* 42 C.F.R. § 160.103 (2013).
[7] *See* 45 C.F.R. § 164.506 (2013).
[8] *See* http://changehealthcare.com/about/investors
[9] *See* http://claimcoalition.org/
[10] J. Bresnick, "Is Blockchain the Answer to Healthcare's Big Data Problems?" (April 27, 2016) at http://healthitanalytics.com/news/is-blockchain-the-answer-to-healthcares-big-data-problems.
[11] I. Aru, "Estonian Government Adopts Blockchain to Secure 1 Million Health Records," at https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records (March 9, 2016).
[12] *See* 45 C.F.R. § 160.103 (2013).
[13] Interview with Gene Boerger, experienced healthcare information technology consultant, on August 3, 2016.
[14] A.M. Antonopoulus, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," 2015.
[15] *See* 45 C.F.R. § 164.514 (2013).