AHLA PG Briefing

The Bridge to Blockchain in Health Care: Guidance for Business Lawyers

Business Law and Governance Practice Group • November 14, 2019

Ty Kayam • Surescripts LLC

Kristen Johns • Waller Lansden Dortch & Davis LLP

AHLA

American Health Lawyers Association

1620 Eye Street, NW
6th Floor
Washington, DC 20006-4010
www.healthlawyers.org
info@healthlawyers.org

Printed in the U.S.A.

This publication is designed to provide accurate and authoritative information with respect to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.
–From a declaration of the American Bar Association.

The application of distributed ledger, or blockchain, technology has permeated many industries. Since its debut through cryptocurrency, many companies have embraced its potential and many more are actively identifying and implementing novel use cases. The health care industry is no different, and blockchain technology is currently being used for physician and nurse credentialing, electronic medical records (EMRs), patient engagement, patient identity, and pharma supply chain management. This article is intended to provide an overview of the current state of adoption of blockchain technology in health care, emerging regulatory and policy implications, and recent guidance that may enable growth and scalability of this technology.

Overview of Blockchain

In the simplest terms, true to its name, blockchain technology involves recording transactions in a database as a "block," and those blocks form a "chain." Each independent database comprising a blockchain network is called a node.[1] Blockchain networks are decentralized, where data is stored by and accessible to all systems that connect to and comprise the network.

Blockchain architectures can vary and have unique characteristics, which can make understanding "blockchains" challenging. As an example, a blockchain network limits who can connect to or access certain transactions stored in the blockchain; this structure is called a *permissioned* blockchain. Permissioned blockchains allow for only a few predetermined nodes to have administrator-type control. Permissionless blockchains allow every node in a blockchain equal access to information in the network in a peer-to-peer fashion.[2] The bitcoin blockchain, for example, is a permissionless, or distributed, blockchain.

[1] *See generally*, *What is a Distributed Ledger?,* https://www.coindesk.com/information/what-is-a-distributed-ledger, https://coincenter.org/learn.

[2] Information can be stored "off-chain," rather than within the block header or the block data, which contain metadata-type information and published transactions, respectively. When information is held off-chain, it is not hosted or accessible to nodes connected to the blockchain network in the manner block headers and block data are accessible, but rather, the information exists in the underlying system of a

Current Challenges

In the United States, the use of blockchain technology in a health care context is not directly regulated. Rather, peripheral laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), establish privacy and security standards for certain health care entities (covered entities and business associates) that create, receive, maintain, or transmit Protected Health Information (PHI). It has been discussed *ad nauseum* that HIPAA, as it is currently structured, is likely the largest obstacle to the commercialization and mainstream adoption of certain applications of blockchain technology involving PHI.

Depending on the use case, a well-functioning blockchain platform will need interoperability among and between covered entities and business associates. However, business associate requirements under HIPAA, such as the requirement to enter into a Business Associate Agreement, do not lend themselves well to the potential applications of blockchain technology. Under HIPAA, a covered entity is required to enter into written agreements with individuals or entities that perform functions or provide services on behalf of the covered entity that involve access to PHI.[3] To comply, covered entities using blockchain technology would need to enter into numerous—possibly thousands or tens of thousands—business associate agreements with various entities accessing information on the blockchain. Further, covered entity and business associate roles blur in a blockchain context. A fundamental characteristic of blockchain is that no one entity has exclusive custody of data. Rather, blockchain technology shifts the current siloed data model to a decentralized (or distributed), synchronized ledger where each entity makes immutable additions to the record. Certain HIPAA requirements, such as return or destruction of PHI or breach notifications, become challenging, if not impossible, to implement.

In addition, blockchain involves the use of mathematically derived pseudonyms for block verification. Mathematically derived pseudonyms pose a problem because HIPAA rules

particular node. Off-chain information can, nonetheless, still be exchanged. *See* https://hackernoon.com/fraud-proofs-secure-on-chain-scalability-f96779574df.

[3] 45 C.F.R. § 164.504(e).

appear to disallow this; the preamble to the Federal Register notice initially implementing the HIPAA regulations in 2002 states:

> Key-hashed message authentication codes are] derived from individually identified information and it appears the key is shared with or provided by the recipient of the data in order for that recipient to be able to link information about the individual from multiple entities or over time.[4]

This may make blockchain technology noncompliant with the re-identification requirements under HIPAA.[5] Also, a covered entity could use a code or another means of record identification to re-identify de-identified information,[6] but that code must remain with the covered entity and must not be capable of identifying an individual.[7] This appears fundamentally incompatible with blockchain technology because more than one entity would need to have access to the code to validate a record.

Regulatory Developments

Three potential developments look promising for blockchain in health care: (1) the prohibition on information blocking; (2) the Trusted Exchange Framework and Common Agreement; and (3) potential changes to HIPAA. In addition, it is worth noting that the National Coordinator for Health Information Technology (ONC) is cognizant of the potential for blockchain in health care.[8] For example, in August 2016, ONC, in tandem with the National Institute of Standards and Technology (NIST), co-sponsored the "Use of Blockchain in Health IT and Health-related Research" Ideation Challenge, soliciting whitepapers on the use of blockchain in health care.

[4] 67 Fed. Reg. 53182, 53233 (Aug. 14, 2002).

[5] Gary LaFever, *Blockchain and big data privacy in healthcare*, IAPP, https://iapp.org/news/a/blockchain-and-big-data-privacy-in-healthcare/ (May 2, 2016).

[6] 45 C.F.R. § 164.514(c).

[7] *Id.*

[8] *See* Announcing the Blockchain Challenge, HealthIT.gov, https://www.healthit.gov/newsroom/blockchain-challenge.

The Prohibition on Information Blocking

The 21st Century Cures Act, signed into law in December 2016, introduced the concept of “information blocking,” defining it as a practice that “interferes with, prevents, or materially discourages access, exchange, or use of electronic health information,” and gave authority to the ONC and the Office of Inspector General (OIG) to combat information blocking practices. The ONC issued a proposed rule in March 2019 on information blocking.[9]

Defining and subsequently prohibiting information blocking activity through this proposed rule is significant because historically health care entities blur the lines between ownership and possession, claiming rights to data in their possession. In fact, HIPAA specifically mandates sharing PHI in two circumstances: (1) upon an individual’s request for his or her PHI, and (2) Department of Health and Human Services (HHS) investigations or HHS’ determination of a covered entity’s compliance with HIPAA.[10] In all other circumstances, sharing PHI is permitted but not required. If the proposed rule is finalized, the information blocking prohibition regulations would mandate sharing health information unless one of seven exemptions applies.[11] This proposed rule could be the impetus for meaningful collaboration among covered entities and other data sources in certain blockchain-based models.

Developers of blockchain networks should note, however, that implementing health information technology in a nonstandard manner that increases the complexity or burden of accessing, exchanging, or using electronic health information (EHI)[12] may constitute information blocking.[13] Specifically, ONC states that “if a particular

[9] 84 Fed. Reg. 7424 (Mar. 4, 2019).
[10] 45 C.F.R. § 164.502(a)(2).
[11] The seven categories of reasonable and necessary practices, and their corresponding conditions, are defined through the exceptions proposed at 45 CFR 171.201–207, and include the following: recovering incurred costs, responding to infeasible requests, maintaining and improving system performance.
[12] Electronic health information is defined as electronic PHI and any other information that is transmitted or maintained by electronic media, which identifies an individual and related to the past, present, or future health or condition of, provision of health care to, or future payment for the provision of health care to an individual. 84 Fed. Reg. 7424, 7513 (Mar. 4, 2019); *see also*, Trusted Exchange Framework and Common Agreement (TEFCA), Appendix 2: Minimum Required Terms and Conditions (MRTCs), Draft 2 published April 19, 2019, page 34.
[13] 84 Fed. Reg. 7424, 7521 (Mar. 4, 2019).

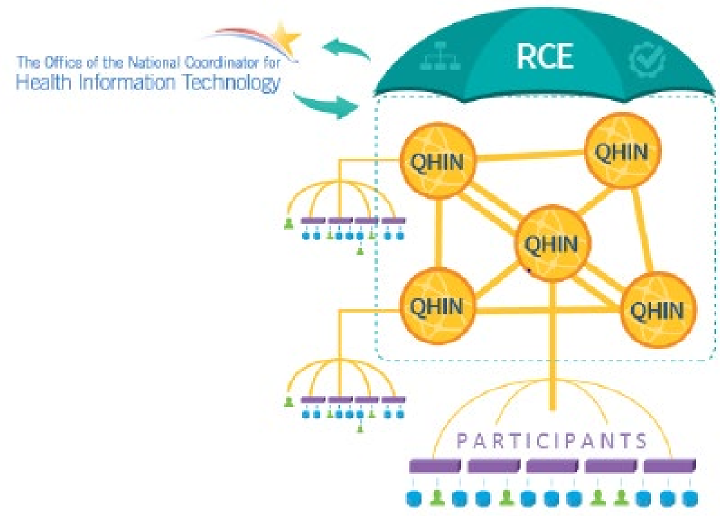
implementation approach has been broadly adopted in a relevant industry segment, deviations from that approach would be suspect unless strictly necessary to achieve substantial efficiencies."[14] ONC and OIG have the authority to decide on a case-by-case basis whether the manner in which technology is developed implicates the information blocking prohibition. For this reason, practitioners should be aware that when designing a blockchain network, the exceptions to the information blocking rules should be reviewed when finalized and measures should be taken to ensure that any final design does not increase the complexity, difficulty, or burden of accessing, exchanging, or using EHI.

The Trusted Exchange Framework and Common Agreement

ONC published a second draft of the Trusted Exchange Framework and Common Agreement (TEFCA) on April 19, 2019. TEFCA consists of principles, terms, and conditions, and a technical framework for the exchange of EHI across siloed health information networks (HINs). Under TEFCA, a HIN can become a qualified health information networks (QHINs), and QHINs form the basis of the Trusted Exchange Framework.[15] QHINs, Participants, Participant Members, and Individuals agree to abide

[14] *Id.*

[15] *See* Trusted Exchange Framework and Common Agreement (TEFCA), Draft 2, published April 19, 2019, page 10:


The Office of the National Coordinator for
Health Information Technology
RCE
QHIN
QHIN
QHIN
QHIN
QHIN
PARTICIPANTS

by a set of rules for the access, exchange, and use of EHI under the oversight of a recognized coordinating entity.[16]

TEFCA is significant for numerous reasons. First, the Exchange Framework has the potential to become the most ubiquitous way to access and share health information. Any entity seeking access to data for specific applications would have the ability to access (currently inaccessible and valuable) health information, opening seemingly limitless opportunities for data-driven organizations to apply novel technologies such as machine learning and artificial intelligence, in addition to blockchain-based use cases. The purpose of the Exchange Framework is to "advance an interoperable health system that empowers individuals to use their EHI to the fullest extent, enables providers and communities to deliver smarter, safer, and more efficient care, and promotes innovation and competition at all levels."[17] A shift in the balance of power in favor of the patient is a simultaneous change to ownership rights previously asserted by entities with control over patient data.

In addition, the TEFCA Draft 2 indirectly acknowledges the application of blockchain technology in the Exchange Framework and associated terms in the Common Agreement. For example, the Minimum Required Terms and Conditions in Appendix 2 includes terms and conditions addressing identity proofing, user authentication, and auditable events.[18] Each of these required elements can be addressed with the application of blockchain technology, yet TEFCA itself does not mandate the application of any specific technology, only suggesting the application of certain NIST standards and specifications.[19] Again, TEFCA outlines the opportunities for data exchange and the terms under which those transactions take place, but does not mandate the application

[16] The Sequoia Project, a health care interoperability not-for-profit, will serve as an RCE.

[17] Trusted Exchange Framework and Common Agreement (TEFCA), Draft 2, published April 19, 2019, page 5.

[18] Exchange(s) Permitted and Future Uses of EHI (§ 2.2.2), Individual Exercise of Meaningful Choice (§ 2.2.3; § 7.3), Onboarding Requirements (§ 2.2.8; § 7.23), Non-Discrimination (§ 5.1; § 8.5), Identity Proofing (§ 6.2.4; § 7.9, § 8.9; § 9.3), User Authentication (§ 6.2.5; § 7.10, § 8.10, § 9.4), Auditable Events (§ 6.2.8; §7.11, § 8.11).

[19] *See* Trusted Exchange Framework and Common Agreement (TEFCA), Appendix 3.

of specific technology. With this guideline and for this purpose, ONC provides a basic framework for new technologies to be adopted and scaled in a meaningful way.[20]

HIPAA Request for Information (RFI)

In December 2018, the HHS Office for Civil Rights (OCR) issued an RFI for potential modifications to HIPAA.[21] Specifically, OCR inquired about encouraging the sharing of information—specifically, PHI—for treatment and care coordination. Currently, HIPAA requires a covered entity to provide a patient's PHI to a third party upon the individual's request within 30 days of the receipt of the request. No such deadline exists, however, for requests that do not originate from the individual. OCR noted that this could lead to instances where medical records are not timely transferred and asked for input on the extent of the problem and potential remedies. Among other issues, OCR additionally inquired whether there should be more rapid reproduction of PHI maintained in electronic media. If an instantaneous requirement is imposed for PHI stored electronically, the distributed nature of blockchain could not only reduce, but eliminate any time gap in the sharing of records.

OCR also contemplates expanding the minimum necessary standard to cover population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development.[22] The "minimum necessary" standard under HIPAA limits certain uses, disclosures, or requests for information to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request.[23] This rule, however, is not universally applicable and some forms of uses and disclosures, such as

[20] Relatedly, the HIPAA Administrative Simplification Rule additionally specifies standards that must be utilized for certain adopted transactions. This means that the blockchain needs to be capable of accommodating and utilizing the identified standards. Alternatively, health information can also be held off-chain whereby the information hosted on the blockchain relates to transactional metadata and all other health information remains in the underlying QHIN or electronic health record system. *See* Sater, Stan, *Blockchain Transforming Healthcare Data Flows* (April 30, 2018). *Available at* SSRN: https://ssrn.com/abstract=3171005.

[21] 83 Fed. Reg. 64302 (Dec. 14, 2018).

[22] 83 Fed. Reg. 64302, 64305 (Dec. 14, 2018).

[23] 45 C.F.R. §§ 164.502(b), 164.514(d).

for a treatment purposes, are exempt.[24] It should be noted that there are more stringent federal and state laws relating to substance use disorder, mental health, and other sensitive information that may impose additional restrictions on how information may be shared.

Other Considerations

In building a blockchain network or platform, developers should consider how role-based access will be implemented. The HIPAA Security Rule limits access to PHI to only those "individuals or software programs that have been granted access rights."[25] The ability to establish a permissioned blockchain network is useful here as it allows for access restrictions, but developers should ensure that removal of access is feasible and determine in advance which nodes should be involved in this process.

One of the underlying tenants of any data usage application is that the output is only as good as the quality and validity of the input (or source data). In health care, input data can originate from the manual input of a treatment event or through sensors, such as monitoring or internet of things (IoT) devices. There is a lot of potential for error with these types of information. As such, efforts should be made to, if feasible, capture and rectify errors within the system or ensure human verification prior to relying on information derived from the blockchain.

Despite certain challenges, blockchain can still be a viable solution so long as developers take into account the current regulations and future modifications to such regulations in building the architecture of the blockchain network. For instance, a consortium or federated blockchain can be considered where only covered entities, rather than business associates, maintain control of the blockchain network. Moreover,

[24] *Minimum Necessary Requirement,* U.S. Dept. Of Health & Human Services, Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html.

[25] 45 C.F.R. § 164.312(a)(1).

to combat the re-identification issue, de-identification can occur off-chain without needing to utilize the blockchain ecosystem.

Conclusion

Although it holds promise, complexity in using blockchain in health care settings remains. The hopeful progress surrounding information blocking prohibitions, TEFCA, and possible HIPAA reforms offer glimpses of a brighter future for blockchain and distributed ledger technology. As regulatory hurdles are removed, a fuller vision for blockchain in health care can emerge and will likely resul in transformative use cases and business models that don’t even exist now.