Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Can Blockchain Deliver Secure IT Solutions For Health Care?

By **Jonathan Gordon and Jesse Welsh-Keyser** (October 16, 2018, 4:01 PM EDT)

Jonathan Gordon

Jesse Welsh-Keyser

It is no surprise to thoughtful commentators that as the hype and prices for cryptocurrencies have waned, functional use cases for blockchain technology have finally taken center stage. For health care, blockchain presents potential solutions to long-standing limitations and frustrations for both providers and patients in both traditional health care and emerging health-related technologies. Blockchain-powered tools may resolve many technical barriers that have prohibited providers from easily exchanging medical and health records while ensuring patients maintain control over when and how their protected health information is shared. And it could potentially empower consumers to control their own biometric, DNA and genomic data with researchers and innovators while enabling the development of new treatments and improving the quality of health care more broadly. But like all technologies with potentially revolutionary applications, blockchain presents novel legal challenges and questions for startups and innovators.

How Does Blockchain Work Again?

At a high level, blockchain is a distributed database or ledger system that can be used to record transactions and even store information. A "blockchain" is made up of a series of shared, immutable "blocks" of encrypted code that are created to reflect a specific set of information and transactions. Once a block is created, it is propagated throughout a network of participants (called "nodes") and then replicated by every node — effectively creating an immutable, "open ledger" for the specific information and transactions memorialized in that block. Each subsequent block (reflecting new or additional transactions or information) is then attached to the block that immediately preceded it, forming an immutable "chain" of permanent blocks.

Blockchain-powered systems can also streamline, or even completely automate, transactions using tools called "smart contracts." The basic premise of a smart contract is to enable participants to create a pre-defined set of terms that must be accepted in order for an automated transaction to occur. Although smart contracts can be far more powerful and complex, a basic example would be predefined rule sets that enable the execution of simple, "if this, then that" transactions.

In blockchain-powered systems, there is no central authority, but instead records and transactions are stored and distributed across all nodes. Information stored on the blockchain — and interactions with

the blockchain itself — are shared to all nodes and require verification by the network before information is memorialized, enabling collaboration between the network participants while recording an immutable audit trail.

Blockchain Use-Cases for the Health Care Industry

Currently, health care providers typically rely on private systems that are used internally within their institutions or networks.[1] Although ongoing standardization efforts are essential to reducing friction when sharing individual patient health information,[2] in many instances providers still rely on cumbersome, often manual processes to receive patient consent and actually share such information with other hospitals and providers.

Using Blockchain-Powered Systems to Enable the Exchange of Medical and Health Information

Much attention has been given to how blockchain technology could provide a decentralized system of information exchanges for medical information, allowing providers to create and access an immutable audit trail that verifies data provenance and also offers increased security — and critical privacy controls — for patients and individuals.[3] Blockchain-powered solutions could be designed to enable compliance with the various regulatory schemes that apply to the health care industry while giving patients and consumers a greater level of control when choosing to share their protected health records and information.

Despite meaningful progress in recent years, substantial technical infrastructure and a myriad of applications must still be built before blockchain-powered solutions can be used to store, intelligently access and allow sharing of digital health information (and other sensitive categories of information, such as genetic information) in a manner that complies with current regulatory requirements.[4] Proponents of blockchain-powered solutions have already proposed many potential solutions. To comply with requirements imposed by the Health Insurance Portability and Accountability Act, some solutions anticipate encrypting sensitive data that is stored on the blockchain (e.g., protected health records), while other proposed solutions would store sensitive data off the blockchain but still use the blockchain network to disseminate “pointers” such as encrypted links or to allow information on-blockchain.[5] The latter approach might expedite adoption by keeping the storage of actual health records off the blockchain and in the hands of trusted health care institutions while allowing access, permissions, authentication and so on to be managed on the blockchain.

Some proposals focus on leveraging smart contracts to automate data management protocols or verify that parties meet predefined requirements or rule sets to share information.[6] An “executed” smart contract could be used to trigger complex data management protocols, including information exchanges with other third-party systems that interface with the blockchain, potentially resolving existing interoperability challenges. Smart contracts could also be used to collect and manage patient consent — and perhaps even automate compliance with certain patient rights imposed by HIPAA or other consumer rights relating to limiting further disclosures and the deletion of certain personal data that would apply to companies that fall outside the scope of HIPAA.

Sharing Biometric, DNA and Genomic Data in Support of Clinical Research and Innovation

Wearable smart devices are becoming ubiquitous and enable the collection of a wide and expanding variety of biometric data. Another exciting use case for blockchain technology is enabling individuals to voluntarily share their own biometric data, health information and even genomic data in support of

clinical research, management of their own health and well-being, and other innovations.[7] By granting medical providers and researchers access to an individual user's biometric data and genome, health care providers, pharmaceutical companies and life sciences researchers can potentially discover and offer new, personalized therapies and drugs. The data-mining and analysis possibilities are endless.

The creation of marketplaces for biometric and DNA data that are documented and secured by blockchain technology have the potential to expand the personalized health care industry. Data shared with researchers could even be supplemented with personal history information ("phenotype" data) to facilitate the analysis of genomic data. However, companies creating these exchanges need to understand the various regulatory regimes that will apply to the gathering, protection and use of this data.

Developing Flexible Solutions for a Shifting Regulatory Landscape

Blockchain-powered technology could revolutionize the IT solutions the health care industry relies on to store and share patient health information and unlock the possibility of leveraging data from consumers to help researchers understand how new treatments can be used. But whether these developments also lead to regulatory crackdowns will depend in large part on whether companies anticipate these issues and complexities in their design and rollout of the first blockchain-powered solutions for the health care industry.

The current laws protecting sensitive health information, such as HIPAA and the California Confidentiality of Medical Information Act, are industry-specific and apply only to certain categories of companies and service providers. Other laws and regulations apply broadly to specific categories of information, such as biometric data or genetic data. For example, the Genetic Information Nondiscrimination Act of 2008 prohibits health insurers and employers from requesting genetic information from individuals or their family members, and GINA also provides legal protections against discrimination on the basis of an individual's genetic information. In practice, this means that individuals who elect to participate in research are protected from insurance and employment discrimination if they choose to contribute their genetic information to studies. GINA does not, however, prohibit discrimination in life insurance, long-term care insurance and disability insurance.

California has just enacted the California Consumer Privacy Act of 2018, which gives consumers additional rights that have been compared to those provided under the EU's GDPR regime. Currently, the CCPA includes an exception for health care companies that are subject to HIPAA, the CMIA or other industry-specific laws, but companies developing solutions for both covered entities subject to HIPAA and other research or commercial customers should anticipate the need to comply with multiple competing regulatory regimes.

As new entrants into the health care industry control access to and sharing of sensitive health and medical information but fall outside the scope of existing laws such as HIPAA, it is only a matter of time before those laws and regulations will be updated or new laws will be passed to specifically regulate these new categories of information holders. Technological advances will continue to make it easier for companies to buy, sell and exchange biometric and genetic data, but the question of who owns the data remains fraught. How will individuals grant and revoke access? What can the data be used for? Where some laws, such as GINA, provide detailed requirements for obtaining informed consent for research purposes, will regulators allow data collected to be repurposed without obtaining new informed consents or providing additional disclosures to patients and consumers?

What's Next: Planning Carefully for the Future

Observers have acknowledged a worldwide trend to place more of the burden on companies and service providers to curb what are sometimes characterized as the trade-offs for innovations in data collection and storage, such as the loss of control by consumers over their own personal data or the increase in targeted commercial marketing. The success of blockchain-powered solutions for health care will be, at least in part, dependent on consumer trust. Consumer reactions to some recent examples of companies facilitating the sharing of DNA information for cross-marketing purposes may provide key insights for companies developing solutions for the health care industry. For example, some commentators have been highly critical of a popular music streaming service's partnership to deliver playlists based on listeners' DNA data, noting that many commercial DNA tests are imprecise and questioning whether the playlists generated have anything to do with genetics at all.[8]

In an era when technology companies in Silicon Valley and elsewhere continue to struggle to find new templates for their leaders, the public has watched as executives from the largest tech companies are summoned before congressional panels and promising biotech startups have failed to deliver results. As state and federal laws and administrative regulations will likely continue to be one step behind innovation, proactively working to maintain consumer confidence and trust will be critical for early market entrants, and companies developing blockchain-powered solutions for the health care industry should consider engaging in collaborative self-regulation and standards development. Such efforts could not only reinforce consumer confidence but also provide an effective roadmap for government regulators as they evaluate if — or more likely, when — to step in. Thoughtful entrepreneurs truly seeking to revolutionize the health care industry with blockchain-powered solutions — not just to gain users, raise capital or scale up their operations — must be ready to confront regulatory complexities head-on and carefully plan for them.

Jonathan Gordon is a partner and Jesse Welsh-Keyser is an associate at Alston & Bird LLP.

[1] See, e.g., Tsung-Ting Kuo, Hyeon-Eui Kim and Lucila Ohno-Machado, Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications, 24 J. Am. Med. Informatics Ass'n 1211 (Nov. 1, 2017), available at https://doi.org/10.1093/jamia/ocx068.

[2] See, e.g., Yichuan Wanga et al., An Integrated Big Data Analytics-Enabled Transformation Model: Application to Health Care, 55 Info. & Mgmt. 64 (Jan. 2018), available at https://doi.org/10.1016/j.im.2017.04.001.

[3] See, e.g., William J. Gordon and Christian Catalini, Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability, 16 Computational & Structural Biotechnology J. 224 (2018), available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6068317/; Alevtina Dubovitskaya et al., Secure and Trustable Electronic Medical Records Sharing Using Blockchain, 2017 AMIA Ann. Symp. Proceedings 650 (2017), available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/.

[4] Id.

[5] See, e.g., Kuo, supra note 1, at 1217.

[6] Id.

[7] See, e.g., Dennis Grishin et al., Nebula Genomics, Blockchain-enabled genomic data sharing and analysis platform (V4.52 Jan. 25, 2018), https://www.nebula.org/assets/Nebula_Genomics_Whitepaper.pdf.

[8] Sarah Zhang, Your DNA Is Not Your Culture, The Atlantic (Sep. 25, 2018), https://www.theatlantic.com/science/archive/2018/09/your-dna-is-not-your-culture/571150/.