

ARTICLE 10

NEW KID ON THE BLOCKCHAIN

By David Kim

In This Article:

Considerations for rolling out blockchain technology for the protection of health and medical data



New Kid on the Blockchain

Over time, advancements in communication have made data and information progressively more obtainable. From medical charts and billing information to test results and clinical trials, the healthcare industry, for one, is certainly not short on data.

In this Information Age, individuals and organizations alike are becoming increasingly reliant on computers and the data, analytics and insights they provide.

But health and medical data are strewn across countless fiefdoms with

very little cross over. Reconciling data scattered across an array of hospitals, clinics, pharmacies, labs and insurance companies is no small feat.

To exacerbate this situation, more and more “things” generating a considerable amount of health and medical data are being added to the internet of things everyday as hospitals are becoming digitally smarter and individuals are using health- and wellness-related mobile apps and wearables.

What Is a Blockchain?

A blockchain is a shared ledger maintained by a distributed network of nodes. The ledger includes a chain of records or “blocks” that are cryptographically linked together.

A consensus is required to add blocks to the ledger. Each node maintains its own copy so that no single node can manipulate the ledger without the others knowing.



Avoiding the Dreaded Data Breach

With all this data, history suggests that it's not a matter of if the data will be breached, but when. And with as much as health and medical data is valued, even the strongest of perimeter security solutions, such as antivirus software, firewalls, and intrusion detection systems, may not be able to keep malicious hackers at bay.

So, how will the healthcare industry continue to leverage—and protect—big data as it accumulates and becomes more fragmented?

Many leaders in the industry believe that blockchain technology may be the solution because of its ability to provide data security, ensure data integrity and facilitate data exchange.

According to a survey published by IBM in 2016, 72 percent of healthcare executives expect to have a commercial blockchain solution by 2020. Some technologists have even predicted that blockchain technology will be more revolutionary than the internet with respect to how we communicate and share data and information.

While many are familiar with Bitcoin, Ethereum and other cryptocurrencies powered by blockchain technology, blockchains can be used to store any type of data or information, such as health and medical data.

Theoretically, blocks could be added to health- and medical-related blockchains by individuals using mobile apps and wearables, as well as healthcare providers, pharmacies, medical device companies, pharmaceutical companies and insurance companies.

Healthcare consortiums could significantly accelerate the advancement of common interests through private, secure and efficient knowledge sharing made possible through blockchain technology.

The industry as a whole would benefit greatly if the right data were available to the right people at the right time.

Blockchains Will Likely Redefine Healthcare Data

Indeed, blockchains may very well redefine how we think of health and medical data. Rather than having healthcare providers store and manage medical records, for example, the patients themselves could manage their own medical records.

Smart contracts with permissions and conditions could be used to selectively authorize doctors to view a

comprehensive history of medical records, which would allow them to provide personalized treatment, and add new records to the blockchain based on the treatment provided.

In addition to medical records, doctors could have access to other data, such as an accurate history of sleep, diet and exercise, that would allow them to have information and insights not previously available, ultimately leading to improved patient care.

Privacy Laws and HIPAA Compliance

While blockchains may be technologically able to address various issues within the healthcare industry, there are other considerations to address, such as compliance with data privacy laws and regulations. Navigating these laws and regulations will be daunting.

Many applicable laws and regulations, like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), were written in an era before blockchain technology. Some have questioned whether blockchains would be HIPAA compliant because of their use of mathematically derived keys – the very thing that allow patients to protect their blockchains. Moreover, the ability for blockchains to remain compliant

with the “Right to Be Forgotten” in Europe under the General Data Protection Regulation (GDPR) may also be in question because blockchains are practically immutable.

One way to address at least some of these concerns is by taking sensitive data off the blockchains while being protected by the blockchains. Blockchains could be used to store, for example, links or pointers to protected health information (PHI), rather than the PHI itself. Moreover, if a large amount of data were taken off the blockchains, data redundancies across the network of nodes would be significantly reduced and a lot of bandwidth could be saved.



What Is a Smart Contract?

A smart contract is a computer program that controls the blockchain. Essentially, smart contracts define the parameters for how a blockchain functions and can set, comply with, and enforce rules for how the blockchain is accessed or used. Smart contracts may be programmed to be self-executing and/or self-enforcing.

Proceed with Understanding and Caution

With its ability to improve data management and interoperability without compromising data privacy, security or integrity, blockchains could be the thing that brings together a fragmented healthcare industry.

Still, as with any new technology, it's likely that laws and regulations will eventually catch up to address novel issues made prevalent through widespread use of blockchains. Businesses should stay updated and remain cautious to ensure compliance with laws and regulations. As with any business decision, it will come down to increasing business value while mitigating risk.

For more information, contact one of the attorneys noted on the right.

Supply Chain Series Contributors



David Kim is an attorney at Stinson Leonard Street. He works closely with his clients to identify business opportunities, protect intellectual property rights and mitigate legal risk. David has extensive experience managing patent portfolios in a broad range of industries, including high tech, telecommunications, financial services, healthcare, energy, aerospace and manufacturing.



Tricia Kaufman, an attorney at Stinson Leonard Street, focuses her practice on the life sciences industry. She counsels medical device and pharmaceutical manufacturers and their vendors, drug compounding outsourcing facilities, healthcare providers, GPOs and others on issues relating to FDA regulations and healthcare compliance laws.



Sheva Sanders practices health law at Stinson Leonard Street. She advises healthcare, managed care, medical device, pharmaceutical, life sciences and PBM clients on complex regulatory issues including fraud and abuse, compliance, reimbursement and transactional matters. She is a frequent teacher, speaker and writer on topics related to health law and health policy.