# Blockchain and Electronic Healthcare Records

By: Nir Kshetri

Kshetri, Nir (2018)." Blockchain and Electronic Healthcare Records ", IEEE *Computer, 51(12), 59*-63.

**Made available courtesy of IEEE: https://doi.org/10.1109/MC.2018.2880021**

## Abstract:

There is a growing need to both secure patient health data from unauthorized breaches and at the same time make access to such data easier for patients. Blockchain may provide a solution.

**Keywords:** Blockchain | Data models | Privacy | Security of data | Hospitals | Insurance | Patient monitoring | Electronic medical records

## Article:

Cyberattacks against healthcare providers pose serious concerns. In 2015 alone, data breaches in healthcare exceeded 112 million records.[1] Current infrastructure cannot guarantee the privacy and security of patient data, and the failure to prevent access to healthcare information by unauthorized persons can harm patients.

The current model of handling electronic healthcare records (EHRs) presents yet another problem: healthcare organizations have shown a tendency to act as custodians or stewards of patient data. This leads to inefficiency and delay in patient care. For instance, a patient’s treatment may be delayed simply because medical information sent from one service provider does not reach another in a timely manner.

Blockchain may offer a solution for addressing current EHR practice limitations. Blockchain initiatives have been implemented by governments, the private sector, and public–private partnership projects. The U.S. Food and Drug Administration (FDA) and IBM Watson Health have teamed up to investigate the potential benefits of blockchain in healthcare; initial efforts have focused on oncology-related data and a blockchain framework.

Blockchain enables the collection of data from a variety of sources and keeps those data in an audit trail of transactions. Blocks hold transaction and other data, and the accountability and transparency of transactions are maintained during this data-exchange process. The FDA and IBM believe that blockchain can support the exchange of data from multiple sources on agreedto terms and for purposes that a patient approves of and consents to. These terms may include EHRs, clinical trials, genomic data, and information gathered from new sources, such as mobile devices, wearables, and Internet of Things devices.[2]

In the blockchain world, permissionless and permissioned chains exist. In a permissionless blockchain such as the open-platform bitcoin, anyone can join. Conversely, private or permissioned blockchains are restrictive, and access must be granted by some authority (e.g., https://www.americanbanker.com/opinion/a-public-or-private-blockchain-new-ethereum-project-could-mean-both). Permissioned blockchains, which are more effective in sharing and managing EHRs, make it possible to share real-time data among participants of healthcare systems and conduct secure transactions. After a transaction is completed by consensus, a permanent record is produced and added to the existing blockchain as a new block (https://tinyurl.com/ycuvnrxw).

In this article, we look at the possible roles of blockchain in strengthening the security and privacy of EHRs and improving efficiency. However, blockchain enforces transparency, which may jeopardize privacy without the proper design considerations.

## CHALLENGES OF THE CURRENT EHR APPROACH

Current EHR models present problems providing efficient healthcare and guaranteeing the security and privacy of patient data. Several of these problems are described in the following.

### Data storage

Current models rely on passwords containing shared secrets that are exchanged and stored on potentially insecure clouds. This approach has led to well-publicized cyberdisasters, such as one in December 2014, where hackers broke into the servers of U.S. health insurer Anthem and stole sensitive information on 80 million customers and employees.[3] Such a breach is less likely to occur in a blockchain model because data are not centrally stored.

### Data sharing

In a nonblockchain world, healthcare organizations typically follow three models to facilitate the interoperability of medical data: push, pull, and view.[4] In a push model, medical information is sent from one provider to another (e.g., from an emergency room physician to a primary care doctor). In a pull model, a provider asks another provider for information (e.g., a cardiothoracic surgeon consulting with a primary care doctor). Finally, in the view model, a provider looks at another provider's patient record. For example, a cardiologist may examine a patient X-ray taken at an urgent care center.

Access to healthcare data must be accompanied by obligations to the data. It is important for healthcare companies handling identifiable information to structure such obligations by associating metadata (i.e., information about information) using data sets.[5] In the current infrastructure, this is more easily said than done. A major drawback of the models describing patient data are that they are not audited in a standardized way. The lack of audit trails means that there is no guarantee of data integrity from the point of data generation to the point of data usage, thus making it difficult to identify the perpetrators of data breaches. Some hospitals still rely on paper medical records and even paper towels.

Fraud is rampant in the medical industry. There have been instances of employees stealing patients' personal data and misusing them (https:// tinyurl.com/y7b8rfta) as well as cases of fraudulent claims submitted to insurance providers using falsified patient medical information and fake identities of doctors. In one scam, employees and doctors at a Long Island-based medical practice defrauded Medicare and Medicaid of US$50 million over a 12-year period by submitting bogus healthcare claims using patients' EHRs (https://tinyurl.com/y9lrhaqt).

Current healthcare systems also fail patients when it comes to informed consent (https://tinyurl.com/yclk4lxd). In the pull model, consent often occurs on an informal and ad hoc basis. Due to time constraints, doctors are often unable to help patients understand the processes related to consent. As a result, patients may not know what questions or whom to ask. It may also not be possible for patients to receive straightforward answers. While patients have the right to stipulate with whom their information may be exchanged, some healthcare organizations lack the capacity to record and implement such stipulations.

### Efficiency

With respect to efficiency, current practice leaves a great deal to be desired. For instance, in the push model, if a patient is transferred to a different hospital, the new hospital may not be able to access the data "pushed" from the first hospital. Patients often feel the frustration of repeatedly supplying the same information to different healthcare providers or different people associated with the same healthcare provider (https://tinyurl.com/y7x83a87).

Current approaches fail to manage medical records generated by multiple healthcare institutions. Because data are scattered across various medical institutions, patient data may become lost (https://tinyurl.com/y7x83a87).

Regulations and policies governing these approaches vary greatly across jurisdictions based on inter alia, local practice, and national privacy policy enforcement. In the United States, laws vary with respect to whether a consent form is required to disclose patient records, the types of medical records patients can access, and procedures for providing patient records to a third party (http://www.apa.org/monitor/jan03/hipaa.aspx).

## BLOCKCHAIN BENEFITS

To understand blockchain's ability to address security and privacy issues (not only related to EHRs), we consider blockchain from the perspective of identity and access management, which involves controlling information such as patient identity on computer networks. The key issues in identity and access management concern 1) information that authenticates the subject's identity, 2) information that describes the information (metadata), and 3) actions that various participants are authorized to know and perform.

The first three rows in Table 1 show current issues related to identity and access management in healthcare that may be improved upon by using blockchain. As previously mentioned, there are drawbacks to existing identity-management techniques that rely on password-based systems. In a blockchain model, a patient's full medical records may be stored in a blockchain ledger's key ring and encrypted using the patient's private key. While a blockchain-based system is not 100% foolproof (e.g., a person's private key can be stolen), it is thought to be more secure than most other current systems.

**Table 1.** Improving security and efficiency in healthcare: Blockchain's potential improvements

| **Key issues in identity and access management** | **Explanation and examples** | **Challenges with the current system** | **Blockchain's potential to address the challenge** |
|---|---|---|---|
| Information authenticating the subject's identity | Information to verify that someone is who he/she claims to be. Examples include a username and password or a thumbprint. | Current identity-management techniques in hospitals rely on password-based systems, which involve shared secrets that are exchanged and stored on insecure systems. | In blockchain-based identity authentication, each transaction needs to be signed by the correct private key. Only the patient has the private key. |
| Information describing the information | Information about different pieces of data flow among participants (e.g., healthcare vendor and patients) and records of data transaction.<br>Information about users' preferences regarding how their data can be used.<br>Consent management records between patients and healthcare services providers. | There are no audit trails of who accessed patients' data. Some hospitals still rely on paper medical records. | The presence of an audit trail means that there is complete documentation of events related to the creation, modification, and deletion of electronic records. |
| Actions that various participants are authorized to perform | An access policy specifies access rights and privileges of each participant. For example, insurance companies cannot have access to patients' confidential medical records. | Various parties are authorized to take actions based on patients' data. Patients often have no control over their own data. | Blockchain prevents unauthorized and illegitimate access to data. Patients hold ownership and ultimate control over their information. |
| Efficiency | Inefficient administrative, logistical, and service delivery processes lead to higher costs, lost time, and fewer benefits.[6] | Inefficient procedures to transfer data across healthcare services providers. Policy and regulatory heterogeneity across jurisdictions. | A consumer has access to her/his up-to-date healthcare information and can forward to a healthcare service provider as and when needed. |

Blockchain offers audit trails, i.e., documentation of the events related to the creation, modification, and deletion of electronic records, thus resulting in transparency. Researchers at the MIT Media Lab and Boston's Beth Israel Deaconess Medical Center proposed MedRec, a blockchain-based decentralized record management system to handle EHRs. MedRec manages authentication, confidentiality, accountability, and data sharing.[7] Using this system, patients can access their medical information from different providers and treatment sites. An immutable log of all transactions involving a patient's information is created and provided to the patient.[7] MedRec does not store patients' health records; rather, its system stores the record's signature in a blockchain. The signature provides assurance that the record's unaltered copy is the one that is obtainable.

Using blockchain, patients hold ownership and ultimate control over their information and decide where their records can travel. In this way, the locus of control is shifted from the institution providing healthcare to the patient. For patients who do not want to manage their data, service organizations may evolve allowing patients to delegate that task to them.[4]

Ensuring that healthcare providers authorize the right person and only the right person is a challenge for implementing blockchain-based models in EHRs in most countries. By adopting a unique digital ID for the identification and authentication of patients, nations can achieve a higher degree of effectiveness for such models. By doing so, they can also improve the quality of healthcare, eliminate insurance fraud, and enhance administrative efficiency.[8]

The bottom row in Table 1 shows how blockchain reduces inefficiency. A key benefit of blockchain-based EHRs is that there is no entity between the patient and his or her medical records. Moreover, there is no need to create custom functionality for each EHR vendor.[4] In the previous example, a patient's treatment will not be delayed simply because medical information sent from a service provider to a hospital was not received; patients can securely share this information with different providers throughout their lifetimes.[4] If there is any change in the patient's condition, the data related to these changes are communicated to the ledger by authorized parties.[9] Thus, timely access to accurate and up-to-date information should improve the efficiency of patient care.

## BLOCKCHAIN CHALLENGES

There are challenges and limitations facing blockchain's management of EHRs. The main barriers to introducing blockchain may be educational rather than technical (http://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers). There has been a general lack of awareness of blockchain's benefits to the medical field.

There are also control- and ownership-related factors, i.e., healthcare providers may encounter barriers that prevent them from moving to blockchain. The psychological challenges healthcare organizations face must be recognized and dealt with so that concerns related to privacy, security, and integrity are addressed. The current mindset among many healthcare providers is that they are the only "steward" of patient data in their respective organizations.[9] It might be difficult to change this culture, but evidence suggests it is necessary. Additionally, not all individuals are in a position to handle their medical data themselves; e.g., older persons or patients with mental illness and dementia may be unable to utilize blockchain to hold ownership and ultimate control over their information.

Furthermore, there are EHR privacy laws such as the Health Insurance Portability and Accountability Act of 1996 that must be enforced (https://tinyurl.com/ydcllwzz). As mentioned previously, blockchain's transparency is not always conducive to privacy. We believe, however, that when appropriate encryption is used for the actual hard patient data and proper control is applied to a specific patient's chain, these two competing forms of trust can occur simultaneously.

There are also scalability challenges associated with blockchains because the size of medical records increases. Using blockchain, a patient's complete medical records must be stored at each node that participates in the network. This may create data-storage and bandwidth problems.[10]

## LOOKING FORWARD

All access to healthcare data should be monitored and logged, and unmonitored access to identifiable information should be prohibited. It may not be realistic or feasible to achieve this goal for current EHR models yet. In many healthcare organizations, mechanisms do not exist to ensure that patient data are not accessed by unauthorized users, and current EHR infrastructure may not meet patient privacy requirements.

These challenges may be addressed with blockchain, which can solve the broader problem of systems relying on password-based security and authentication. The blockchain ledger includes an audit trail and data that are time-stamped, which allows the patient to know (within reason) who made what changes and when. Third parties such as healthcare providers can see patient data with the patient's permission, but they are not required or expected to store the data. In this way, a blockchain-based model is superior to existing data-governance models.

In recent years, significant initiatives have been undertaken in a range of settings that use blockchain to strengthen the security and privacy of healthcare data. The main focus of many of those initiatives has been on audit trails. Blockchain may also lead to more efficient healthcare practices by addressing existing inefficiencies that cause lost time, poorer care, and higher costs.

## ACKNOWLEDGMENT

I thank Jeff Voas for his contributions to this article.

## REFERENCES

**1.** D. Munro, *Data breaches in healthcare totaled over 112 million records in 2015*, 2015, [online] Available: https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#5a1974687b07.

**2.** F. Bazzoli, *FDA IBM Watson Health to study application of blockchain technology*, 2017, [online] Available: https://www.healthdatamanagement.com/news/fda-ibm-watson-health-to-study-application-of-blockchain-technology.

**3.** A. W. Mathews, D. Yadron, *Health insurer Anthem hit by hackers*, 2015, [online] Available: https://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

**4.** J. D. Halamka, A. Lippman, A. Ekblaw, *The potential for blockchain to transform electronic health records*, 2017, [online] Available: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

**5.** P. M. Schwartz, D. J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information", *New York Univ. Law Rev.*, vol. 86, pp. 1814-1894, 2011.

**6.** H. de Koning, J. P. Verver, J. van den Heuvel, S. Bisgaard, R. J. Does, "Lean Six Sigma in healthcare", *J. Healthcare Quality*, vol. 28, no. 2, pp. 4-11, 2006.

**7.** A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, *A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data*, 2016.

**8.** The role of digital identification for healthcare: The emerging use cases, Washington, D.C:The World Bank, 2018, [online] Available: http://pubdocs.worldbank.org/en/595741519657604541/DigitalIdentification-HealthcareReportFinal.pdf.

**9.** L. Silverman, *How bitcoin technology could securely share medical records among your doctors*, 2017, [online] Available: http://keranews.org/post/how-bitcoin-technology-could-securely-share-medical-records-among-your-doctors.

**10.** L. A. Linn, M. B. Koo, *Blockchain for health data and its potential use in health IT and healthcare-related research*, 2016, [online] Available: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf.