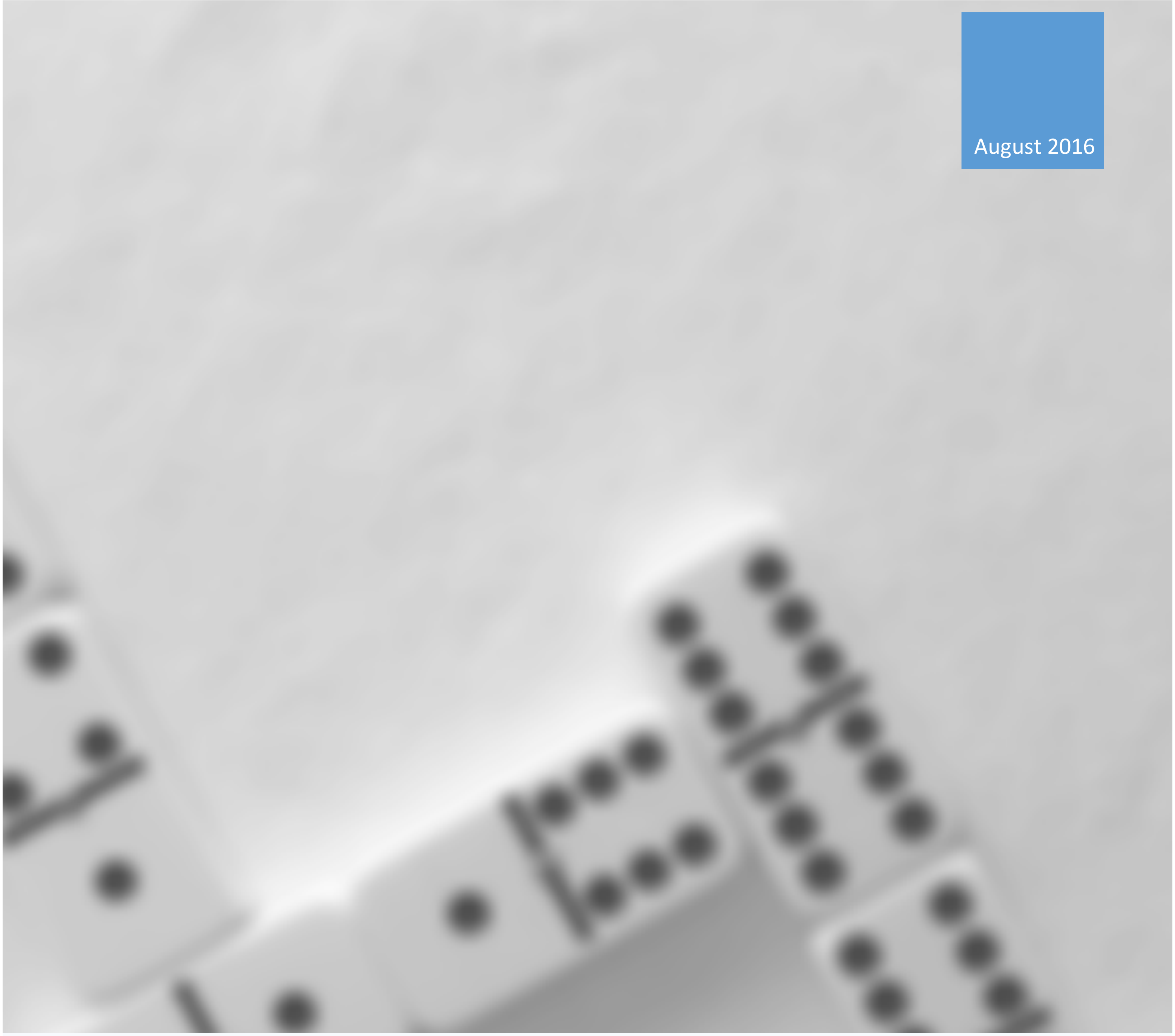
August 2016



# Moving Toward a Blockchain-based Method for the Secure Storage of  Patient Records

Drew Ivan
drew.ivan@gmail.com

## Abstract

Today's methods of recording and sharing patient data have a number of limitations that restrict patients' access to their clinical records, reduce availability of essential data to care providers, and ultimately present a barrier to transforming U.S. healthcare into a learning health system. Storing patient healthcare data in a blockchain-based storage scheme can remediate these shortcomings. This paper discusses blockchain as a novel approach to secure health data storage, implementation obstacles, and a plan for transitioning incrementally from current technology to a blockchain solution.

## Overview of Today's Environment

As recently as 2008, less than 10 percent of medical records were stored electronically (Figure 1)[1]. Paper based records are difficult to move or copy from their original location to other places of service or directly to the patient. Today, nearly all medical records are stored in electronic health record (EHR) systems, yet data remains largely non-portable.

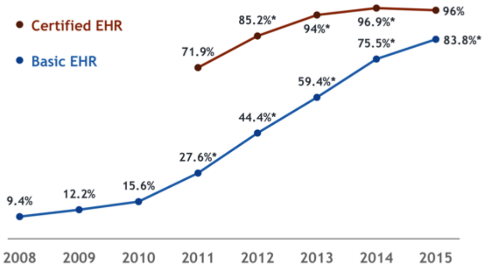


*Figure 1. Adoption of Electronic Health Records in Federal Acute Care Hospitals*

Several factors contribute to the difficulty of providing and controlling access to healthcare data. Many healthcare providers err on the side of caution when interpreting HIPAA requirements[2], sharing data only when absolutely required. This extends to restricting patients and their proxies from accessing data about their own health. Some institutions perceive data stewardship as a competitive advantage. Owning the patient's medical record promotes "stickiness," while sharing it allows the patient to seek care from another institution. Healthcare providers perceive the patient's medical record as their property rather than the patient's. While this is true in a legal sense[3], it creates unnecessary and sometimes costly obstacles for patients that need or want to move their medical records to another location.

Meaningful Use, the program responsible for the fast adoption of EHRs in the past seven years, requires that providers enable patients with the capability to view, download, and transmit their records to other locations[4]. Most providers today are sharing at least some data with external systems[5], indicating limited progress in this area; however, the status quo remains that information generally stays in the system that generated it. This is a significant enough problem that the Office of the National Coordinator has adopted procedures to identify and correct instances of "information blocking."[6]

The difficulty in securely moving and sharing health data in a timely manner has detrimental impacts on patient care.

In a 2008 essay[7], Doc Searls relates a personal anecdote that describes the type of impact that poor record sharing can have on patient treatment. His conclusion is that patients need to be in control of their healthcare, and that includes controlling their healthcare records. In his words, the patient needs to become the platform for healthcare, but "for patients to become platforms, we need more tools and capabilities that are native to the patient." Searls goes beyond stating that electronic health data should be easy to share; he advocates making patients the custodians of their own healthcare data, so that they ultimately control where and how it can be used.

As adoption of electronic health records increases, failing to execute on the promise of sharable health data is not the only problem facing EHR systems. Broader adoption of electronic health records has enabled previously unknown levels of health data breaches[8] (Figure 2).

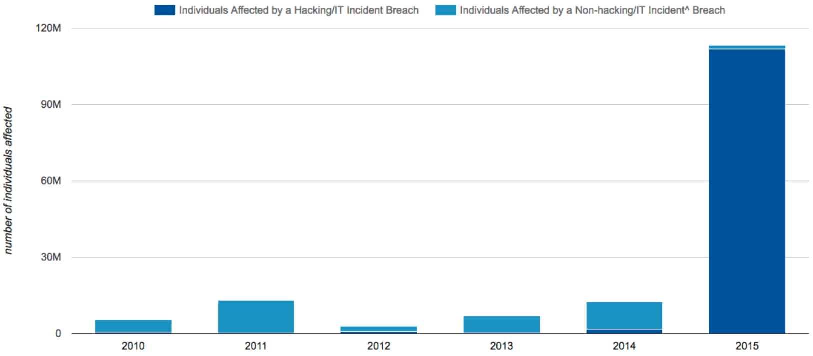


*Figure 2. Number of individuals affected by health information breaches*

A majority of patients are concerned about privacy and security of medical records, and some patients withhold information from their healthcare provider because of these concerns[9].

Widespread adoption of electronic health records needs to be a secure, trusted and efficient solution to the problem of being unable to share data among providers, patients and researchers. Instead, the information silos are nearly as impenetrable as they were in the days of paper records, with the added risk of frequent, high impact data breaches.

## Blockchain-based Medical Record Storage and Data Exchange

A possible solution to these (and many other) issues is the implementation of a patient controlled, blockchain-based system for clinical record maintenance and sharing. To understand how blockchain technology can improve the security and efficiency of electronic health data storage and sharing, it is first necessary to provide an overview of blockchain technology and its benefits.

Blockchain technology rests on three foundational tenets[10]. First, data is stored in a public, immutable transaction ledger that anyone can read. Because the transactions can never be deleted or changed, there is always a complete and irrefutable record of all transactions. Second, blockchains are implemented in a decentralized network of computing nodes, which makes them robust against failures and attacks. Decentralization also means that no entity owns or controls the blockchain. Third, the metadata describing each transaction is available to everyone on the system, but that does not mean the data stored within the blockchain is readable. Blockchain relies on pseudoanonymity (replacing names with identifiers) and public key infrastructure (PKI), which allows the blockchain's contents to be encrypted in a way that is prohibitively expensive to crack. When applying blockchain technology to health data, each of these foundational tenets applies.

### Immutable Transaction Ledger

Blockchain was originally conceived as an infrastructural component of the cryptocurrency, Bitcoin. The transactions on Bitcoin's blockchain represent financial transactions: moving specific amounts of Bitcoin from one account to another. Anyone can verify which account a particular Bitcoin belongs to by using appropriate software tools to examine the transactions on the public blockchain.

In a healthcare context, transactions would consist of documentation of specific episodes of healthcare services provided. Healthcare providers, payers and patients would contribute encrypted data, which would reference a patient ID, to a public blockchain. This could include clinical data that is stored in EHR systems today; claims history and gaps in care from payers; and family history and device readings from patients. This information would be encrypted and stored in the blockchain and could only be decrypted by parties that have the patient's private key[11]. (Figure 3).

Because the ledger is immutable, no one can erase or alter the record. Updates include metadata records of the date, time, location and entity making the update. In this way, a blockchain-based medical record will be self-auditing.

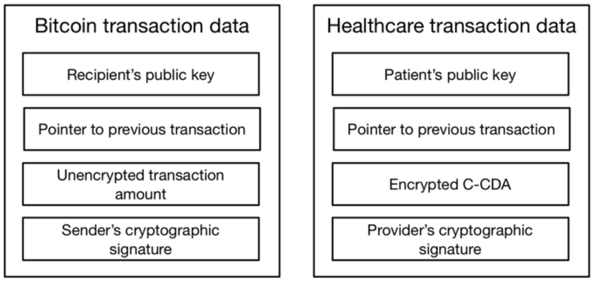

Bitcoin transaction data
Recipient's public key
Pointer to previous transaction
Unencrypted transaction amount
Sender's cryptographic signature
Healthcare transaction data
Patient's public key
Pointer to previous transaction
Encrypted C-CDA
Provider's cryptographic signature

*Figure 3. Example of financial versus healthcare blockchain transactions*

## Distributed Network

Financial, legal, healthcare and other types of transactions have some common requirements. It is necessary to establish the identities of the parties involved in the transaction, maintain trust, ensure that transactions are recorded properly and cannot be altered, and that the infrastructure in which transactions occur is stable. Prior to blockchain, the only way to achieve these goals was to establish a strong central authority to provide these services, for example banks, governments and clearinghouses. In the domain of health records, each hospital or health system serves as its own central authority to provide record keeping and transmission services.

The traditional, centralized transaction infrastructure is a natural solution to the problem. While it has many advantages, there are also drawbacks. A centralized infrastructure is vulnerable to failure, corruption and attack. This architecture causes the information silos that are prevalent in healthcare today.

Blockchain replaces the centralized infrastructure with a distributed one. The blockchain software is running on thousands of nodes distributed across an entire network. To process a transaction, it is distributed to all the network nodes, and the transaction is cleared when the nodes have reached a consensus to accept the new transaction into the common ledger.

The process is technologically sophisticated, but it replaces entire record keeping and transaction processing institutions. This lowers transaction overhead in terms of price and execution time. It also means there is no single point of failure, providing a more robust, safer infrastructure.

## Strong Encryption

Public Key Cryptography is an encryption system that uses pairs of keys: a "public key" available to everyone and a "private key" that is known only to its holder. Either key may be used to encrypt a message, but the other key must decrypt the message. Practically speaking, there are two use cases involving public and private keys. First, a sender can encode a message with a public key and be sure that only the holder of the private key can decrypt it. Second, a message or document can be encrypted with a private key. If the message makes sense when it is decrypted using the corresponding public key, it's guaranteed that the holder of the private key is the party that encrypted the message. This is sometimes called "signing" a message[12] because it is analogous to someone putting his unique signature on a document.

Blockchain also supports a concept called *M*-of-*N* signatures or "multisig," meaning that there are a total of *N* cryptographic keys, and at least *M* of them have to be present in order to decrypt the data. In this way, the patient can provide keys to authorized caregivers, doctors and others to grant access without the patient's specific key[13]. For example, this is useful when the patient is incapacitated and cannot provide consent to access the data.

Public Key Cryptography is an important concept for blockchain. All transactions are signed with private keys as a way of establishing the participants' identities. In the context of storing healthcare data in a blockchain, cryptography would have the additional role of encrypting the contents of the message, so that only intended users can read its contents.

## Implementing a Blockchain Solution

To implement a blockchain-based healthcare record system, EHRs and other record keeping systems would encrypt and send a transaction containing patient care documents – encounter notes, prescriptions, family histories, etc. – into the public healthcare blockchain. The transaction would include a digital signature from the contributor to trace provenance and the patient's blockchain ID as the recipient of the transaction.

After the documents are stored in the blockchain, patients would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties.

This type of system has a number of advantages over current methods of record keeping:

1. Patients becomes the platform, owning and controlling access to their healthcare data. This removes all obstacles to patients acquiring copies of their healthcare records or transferring them to another healthcare provider.
2. Because data is stored on a decentralized network, there is no single institution that can be robbed or hacked to obtain a large number of patient records.
3. Data is encrypted in the blockchain and can only be decrypted with the patient's private key. Even if the network is infiltrated by a malicious party, there is no practical way to read patient data.
4. The infrastructure itself provides auditing and non-repudiation capabilities. The methods used to add the data to the blockchain also include tamperproof timestamps, account IDs, and methods of determining if the contents have been altered.

A blockchain-based method of storing healthcare data includes all the expected criteria of a medical record keeping system, and it goes beyond what a traditional, centralized system can do because it improves patients' access to their records and strengthens security against data breaches.

## A Practical First Step

It is naïve to think that the healthcare industry will discard today's solutions and re-implement its recordkeeping systems on a blockchain architecture. Healthcare is a risk-averse industry, unlikely to readily accept the time and cost required to shift to a new and unproven technology. In addition, there is a great deal of inertia and investment in the status quo.

To achieve high rates of EHR adoption, the Centers for Medicare & Medicaid Services (CMS) has spent over $30 billion since 2011[14]. A new approach to recordkeeping will need to respect this investment and work alongside the existing EHR infrastructure, not supplant it. The institutions that are maintaining healthcare data in centralized systems perceive patient data as a valuable asset, and it will be difficult to change their way of thinking.

While a blockchain-based solution may be an option at some point in the future, the near-term requires a bridge solution. The following, proposed solution includes creating a new facility for storing clinical data that is based on blockchain technology, while continuing to use today's EHR (and other) systems to capture and store patient data. This provides many of the advantages of the blockchain solution, while leveraging current healthcare IT investments. Existing standards and policies provide the framework for copying data from traditional systems into the new, blockchain-based system. The new system will effectively be a blockchain-based personal health record (PHR).

The proposed solution begins with today's health IT systems, primarily EHRs, but also potentially includes laboratory information systems, radiology systems, payer databases, medical devices and consumer devices. These systems will continue to operate as they do today, storing data in their proprietary databases. In addition to storing its own copy of the data, each system will also transmit a copy to the blockchain-based PHR.

All EHR systems that are Meaningful Use compliant must provide the ability for patients to view, download and transmit their health information in human readable as well as machine readable format[15]. The document format is C-CDA, a machine-readable XML format. By applying a style sheet to the C-CDA document, it becomes an HTML file that can be read by a human using a web browser.

Many health systems satisfy the view/download/transmit criterion by making C-CDA documents available to the patient on a patient portal. From there, the patient can download or forward the document to the destination of their choice. Some EHR systems also offer other methods of transmission that do not require a patient portal.

There are three options for connecting an EHR's view/download/transmit function to a blockchain-based PHR:

**Option 1:** EHR vendors implement a blockchain client within their EHR software that communicates health information directly and automatically to the blockchain-based PHR. (See Figure 4 below.) This would be the preferred option, but it requires effort and cooperation on the part of EHR vendors and is unlikely to occur without regulation or incentive.

**Option 2:** EHR vendors use existing protocols, such as REST, SOAP or Direct Messaging to send health information to a blockchain-based PHR, which is equipped to receive data according to these standards. This would mean that the blockchain-based PHR would need to be able to handle these communication protocols and configured to receive documents from various sources. Such functionality is somewhat heavyweight for a blockchain-based system, which is conceived as a simple electronic transaction ledger.

**Option 3:** Patients continue to receive their health information through existing patient portals and then forward or upload the documents to the blockchain-based PHR. This "lowest common denominator" method will work in all cases, but it relies on the extra, manual step of the patient acting as an intermediary. In a worst-case scenario, this will result in incomplete records if the patient does not complete the manual step.

Option 3 is the simplest scenario and the easiest to implement. The feasibility of the other two options depends on the willingness of EHR vendors.

For systems other than EHRs, the situation is somewhat less clear. Conceptually, there are ways to split the stream of data coming out of these systems and send a copy to the blockchain-based PHR; however, the economics and regulatory issues involved may complicate and delay the implementation of these efforts.

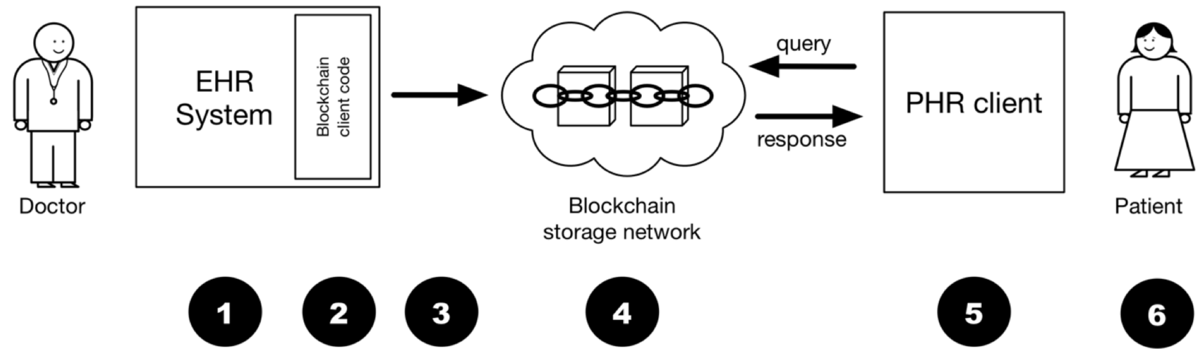


*Figure 4. Architecture and data flow for the EHR with built-in blockchain client (option 1).*

1. *Upon completing an encounter, the EHR saves data locally, prepares a C-CDA version of the encounter data, and transfers it to the built-in blockchain client.*
2. *The built-in blockchain client encrypts the document using the patient's public key and connects to the blockchain to transmit the document.*
3. *The C-CDA document, along with metadata about the document's source and subject, is committed as a transaction to the blockchain. The nodes of the blockchain network use a consensus algorithm to determine the transaction's validity, and when a quorum of nodes agrees to the change, it is permanently committed to the public ledger.*
4. *The blockchain stores all documents for all patients.*
5. *The PHR client is able to connect to the blockchain and download all documents for the patient. The documents are decrypted using the patient's private key.*
6. *The patient is able to view the documents and share them with other providers.*

## Other Considerations

A healthcare data recordkeeping system that is fully based on blockchain technology is possible, but not practicable in the near future. The bridge strategy of a blockchain-based PHR existing alongside the current healthcare data infrastructure is more realistic, yet there remain significant obstacles and challenges to overcome.

The first challenge is that a suitable blockchain infrastructure for healthcare does not currently exist. More importantly, there is no clear stakeholder who seems motivated to create one.

In order to establish and maintain a network of worker nodes, it is necessary to incent individuals and organizations to dedicate their computing power. The nodes that maintain the Bitcoin blockchain are rewarded by being able to "mine" new bitcoins that are deposited in the node owner's account.

What would motivate computer owners to use their processing power to maintain a healthcare blockchain?

One suggestion[16] has been that the nodes contributing data to the system would also supply the compute power to maintain the healthcare blockchain. This is feasible, but if the contributors are hospitals and healthcare systems, the total number of nodes in the network may be fairly small. A robust blockchain relies on a large number of independent nodes. This also means that the central authorities that currently control data silos would remain in charge of the infrastructure, derailing the concept of putting trust in the network rather than a small number of central authorities to keep the data safer and more secure.

A further consideration is that the blockchain infrastructure storing the data has to be invisible to the end users – both patients and healthcare providers. The storage technology needs to be abstracted by the user facing tools. If a user has to take time-consuming extra steps to work with data in a blockchain, widespread adoption could be at risk.

Performance is a major technical consideration for any blockchain-based solution. Depending upon the implementation details, performing large numbers of transactions on a blockchain can be very expensive in terms of time and processing power. This means that performance and scalability need to be designed into the designed into the solution from the start.

## Alignment with ONC's Interoperability Roadmap

*Connecting Health and Care for the Nation: A shared Nationwide Interoperability Roadmap,*[17]published by the Office of the National Coordinator in late 2015, lays out a path toward a learning health system, in which information flows automatically among stakeholders within the healthcare system. Its wide-ranging components are organized into 15 broad categories. A blockchain-based PHR supports a number of these efforts as summarized below. (Not included: Roadmap items that the envisioned blockchain solution does not directly.)

**Roadmap Item A: Supportive Payment and Regulatory Environment**

For patients whose data is stored in the healthcare blockchain it will be possible for payers to implement smart contracts[18], executable business rules that run within the context of a blockchain. A smart contract could be attached to a patient's record that responds, when queried by a properly credentialed source, to the question of whether the patient's record contains evidence that his care has met the quality standards set forth by the payer. For example, the payer could ask the blockchain, "If the patient has a diagnosis of type 2 diabetes, has he received a retinal screening in the past year[19]?" The smart contract would answer yes, no, or not applicable. In this way, quality measurements can be automatically calculated without disclosing any personal information.

Smart contracts have the potential to dramatically simplify and automate payment schemes based on quality measures.

**Roadmap Item B: Shared Decision-Making, Rules of Engagement and Accountability**

A blockchain-based PHR is a perfect way to bridge the gap between HIEs that operate using different standards and in different geographies. The ability for smart contracts to expose the minimum amount of data necessary to satisfy a query also has applicability for non-healthcare users to interrogate the blockchain.

**Roadmap Item C: Ubiquitous, Secure Network Infrastructure**

While a blockchain-based PHR has very little to do with whether technology vendors and healthcare organizations adopt cybersecurity best practices, it is certain that those best practices would inform the system design and implementation. By adopting a blockchain-based PHR, organizations could rest assured that their PHR strategy complies with the ONC's roadmap recommendations.

**Roadmap Item D: Verifiable Identity and Authentication of All Participants**

While a blockchain-based PHR does not, itself, contribute toward this goal, it would be able to work well with an identity system, such as a security token, to establish user identities when accessing the blockchain[20].

### Roadmap Item E: Consistent Representation of Authorization to Access Electronic Health Information

Like roadmap Item D, the blockchain-based PHR does not directly contribute to this goal; however, with the patient having more control over his own medical records, authorization standards will be increasingly important in carrying out the patient's wishes regarding usage of the record.

### Roadmap Item F: Consistent Understanding and Technical Representation of Permission to Collect, Share and Use Identifiable Electronic Health Information

A blockchain-based PHR is well suited to implementing restrictions based on a patient's privacy preferences. In fact, smart contracts could automate the process of informed consent. For example, a patient could create a smart contract that provides anonymized data about his tumor biopsy to any research organization that asks for it. This would happen automatically, without the patient having to explicitly release the information.

### Roadmap Item I: Consistent Data Formats

A blockchain-based PHR would initially be based on C-CDA documents generated by EHR systems. In that respect, it relies upon and reinforces the structural standard in place. The blockchain-based PHR does not specifically further the goal of standardizing on vocabularies and code sets.

### Roadmap Item J: Secure, Standard Services

A blockchain-based PHR would be a vital participant in an API-based health IT ecosystem; however, the PHR does not specifically facilitate the adoption of APIs.

### Roadmap Item K: Consistent, Secure Transport Techniques

With its use of public key cryptography, a blockchain-based PHR, communicates using a secure transport protocol. If such a system gains widespread adoption, it could supplant protocols (such as Direct Messaging) as the preferred method of transferring healthcare data.

### Roadmap Item N: Individuals Have Access to Longitudinal Electronic Health Information, Can Contribute to that Information, and Can Direct It to Any Electronic Location

The concept of patients being able to access, contribute to, and direct the movements of their healthcare data is not new, nor is it fully realized. Easily accessing and moving data was difficult prior to the widespread adoption of electronic medical records for logistical reasons. Even now that the vast majority of medical records are stored electronically, there is very little progress in the area of consumer-mediated HIE[21].

The barriers to consumer-mediated HIE are cultural, economic, and technical. A blockchain-based PHR is the perfect solution for the technological aspect of this roadmap item. A perfect technological solution can pave the way for changing culture and economy as well, similar to when the technology of online digital music services led to changes in the economics and culture of the music industry.

### Roadmap Item O: Provider Workflows and Practices Include Consistent Sharing and Use of Patient Information from All Available and Relevant Sources

A blockchain-based PHR will play a critical role in realizing this roadmap item. As a central repository for patient data, it makes sense to embed it into provider workflows. For example, a provider's EHR might automatically query the blockchain-based PHR for relevant records when a patient record is opened. This would give the provider a view into data about the patient collected outside of his local EHR. When an episode of care is complete, the provider's EHR would automatically contribute a care summary to the blockchain-based PHR.

### Roadmap Item P: Tracking Progress and Measuring Success

A blockchain-based PHR is well positioned to report on the amount of traffic into and out of the blockchain. It could even provide granular reports that break down interoperability by region, data type, etc. A blockchain-based PHR can not solve the interoperability measurement problem for interoperability technologies other than itself. It will be able to provide detailed reports of its activity from a central location, a differentiator from other technologies.

## Conclusions

Recent years have seen a dramatic rise in the adoption of EHR technology, yet the promise of secure, easily transported electronic patient data remains elusive. Blockchain technology has the potential to solve the problem by providing a single, secure, decentralized storehouse of clinical data for all patients. A stepping stone toward this goal is to implement a blockchain-based PHR where, using existing Meaningful Use standards, authorized entities receive a copy of patient data.

Such an approach allows patients better access to and control over their health data, including the ability to contribute to their record, send it to any care setting they desire, or share parts of it with research organizations, including projects related to initiatives like PCORI and the Precision Medicine Initiative (PMI).

## References

Mougayar, William. *The Business Blockchain.* Hoboken, NJ: John Wiley & Sons, Inc., 2016.

Personal health record. (2016, July 28). In *Wikipedia, The Free Encyclopedia*. Retrieved 01:31, August 2, 2016, from https://en.wikipedia.org/w/index.php?title=Personal_health_record&oldid=731937216

Public-key cryptography. (2016, June 29). In *Wikipedia, The Free Encyclopedia*. Retrieved 01:30, August 2, 2016, from https://en.wikipedia.org/w/index.php?title=Public-key_cryptography&oldid=727484910

Swan, Melanie. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, Inc., 2015.

Tapscott, Don and Tapscott, Alex. *Blockchain Revolution.* New York, NY: Penguin Random House LLC, 2016.

## Endnotes

[1] http://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php

[2] http://www.nytimes.com/2015/07/21/health/hipaas-use-as-code-of-silence-often-misinterprets-the-law.html?_r=0

[3]http://www.andersonhunterlaw.com/about/news/archives/2011/02/01/who_owns_your_healthcare_information

[4] https://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures-2/patient-ability-electronically-view-download-transmit-vdt-health-information

[5] http://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-interoperability-2015.php

[6] https://www.healthit.gov/buzz-blog/from-the-onc-desk/health-information-blocking-undermines-interoperability-delivery-reform/

[7] http://www.linuxjournal.com/content/patient-platform

[8] http://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php

[9] http://dashboard.healthit.gov/evaluations/data-briefs/trends-individual-perceptions-privacy-security-ehrs-hie.php

[10] https://www.linkedin.com/pulse/title-blockchain-healthits-cyber-superhero-drew-ivan

[11] https://www.linkedin.com/pulse/aggregation-through-decentralization-drew-ivan?trk=pulse_spock-articles

[12] More accurately, a message’s mathematical summary, or hash, rather than the whole message, is typically signed with a private key.

[13] https://www.linkedin.com/pulse/blockchain-technology-solution-healthcare-peter-b-nichol

[14] https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/dataandreports.html

[15] https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_7_PatientElectronicAccess.pdf

[16] http://geekdoctor.blogspot.com/2016/03/evaluating-blockchain-for-health.html

[17] https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[18] http://szabo.best.vwh.net/smart_contracts_idea.html

[19]https://www.qualitymeasures.ahrq.gov/summaries/summary/48828/comprehensive-adult-diabetes-care-percentage-of-patients-18-to-75-years-of-age-with-type-1-or-type-2-diabetes-who-had-an-eye-exam-retinal-performed

[20] https://www.youtube.com/watch?v=2V0XqKb9nhg

[21] http://blogs.wsj.com/experts/2016/06/28/how-to-make
-health-care-records-as-mobile-as-patients/