Healthcare Record Modernization through the Application of Blockchain

Author team; Rudy Bochek (TESCHGlobal), Antonio Fernandez (TESCHGlobal), Hadrian Zbarcea (apifocal), Will Tesch (HealthLX)

Introduction

This paper proposes a healthcare model for blockchain that addresses nationwide interoperability challenges to aggregate disparate distributed Healthcare records securely and privately. The approach we're recommending isn't revolutionary by itself, instead our recommendation of the implementation of blockchain further builds upon the nationwide interoperability foundational goals.

"Establish a coordinated governance framework and process for nationwide health information interoperability....To enable nationwide interoperability for a common clinical data set, there must be agreement on the policies, operations and technical standards that ***will enable trust*** *and allow information to be shared appropriately across the ecosystem."* ~ ONC Interoperability Roadmap (pg 12, pt. 1)

Said another way...for our healthcare system to reach interoperable efficiency "Trust" must be established between the parties involved in the health care lifecycle, Patients, Providers and Payers. Without "Trust" between these parties, sharing and interaction of healthcare data cannot mature over time. Blockchain enables 'Trust' unlike any data encryption and storage technology introduced in human history. This paper focuses on our recommended implementation of Blockchain.

Setting the stage - ONC Guidance and Pledge

On February 29th, 2016 ONC Secretary Burwell announced the Interoperability Pledge made by EHR vendors that made up 90% of the EHR record storage in the United States. There were three core features to the commitment [1]:

1. ***Consumer Access:*** *To help consumers easily and securely access their electronic health information, direct it to any desired location, learn how their information can be shared and used, and be assured that this information will be effectively and safely used to benefit their health and that of their community.*
2. ***No Blocking/Ensuring Transparency:*** *To help providers share individual's' health information for care with other providers and their patients whenever permitted by law, and not block electronic health information (defined as knowingly and unreasonably interfering with information sharing).*

3. ***Standards:*** *Implement federally recognized, national interoperability standards, policies, guidance, and practices for electronic health information, and adopt best practices including those related to privacy and security.*

While each of these three points is broadly accepted by the healthcare community, the implementation of the pledge doesn't speak to a driving technology that would embrace the concept overall. Instead the means to accomplish the pledge has been left to the public / private sectors to solve. Modern Healthcare has been a beneficiary of advancements in technology and standards of the past such as contributions by the HL7 community.

The HL7 consortium published a set of standards for recording healthcare related data. Unfortunately they were not systematically standardized across the EHRs which is so common to the highly-specialized healthcare industry. More recently HL7 developed the C-CDA standard enabling a means to organize commonly recognized care information into a common document. In response to and in collaboration with the Office of the National Coordinator (ONC), there has been sponsored innovation to continue with the need to view CCD information from disparate systems in a commonly viewed way. *(The authors of this article recently placed 2nd in the CCD Viewer contest sponsored by ONC and HL7)*

Our proposition in this paper addresses the above past achievements and in particular embraces the advances with the C-CDA standards, but also respects the adoption rate of standards. We believe today's reality is best described as the work-in-process of the learning health system [2] while embracing the value of the ONC vision and roadmap overall. As a reference, let's assess the nature of interoperating with patient data with a provider encounter in today's view.

Today: short-story on personal healthcare data distribution

From a patient view, it has long been established that our personal health information, which resides in our doctor's office or provider's EHR, is our 'personal' information. While this may be accurate, these records are observations whether subjective through documented doctor's notes or more objective through lab results or specialized procedures such as x-rays. These observations once stored digitally tell a story about our encounter that reside in an EHR system or supporting specialized applications. The operational storage capabilities of the EHR software to arrange the data is broadly considered their competitive advantage between the various EHR software solutions. But the arrangement of the encounter observation data is not a competitive differentiator for interoperability, instead the ability to digitally share the patient encounter (CCD) or collection of historical encounters outside of the EHR system has been agreed to be the single unifying definition of patient data interoperability. As a Meaningful Use 2 requirement, this patient health data is now available for distribution in a standards format

which will likely continue to evolve (currently C-CDA specifications v2.1), although adoption has been slower than expected.

Even though this information is available and required by law [3] factors that make this information less than sufficiently 'shareable' outside the provider's network include:

1) Resistance to share due to HIPAA interpretation and liability as understood by the EHR user.
2) Lack of clear permissions by the requesting parties needed to see the information
3) Reliance on accurate and reliable interpretation of encounter information by sending party to receiving party
4) Process acceptance and reliability by providers or actors in the transmission process
5) Lack of a means to authenticate permission of PHI use by patient.
6) Overall lack of knowledge of how to implement the C-CDA architecture at the providers.

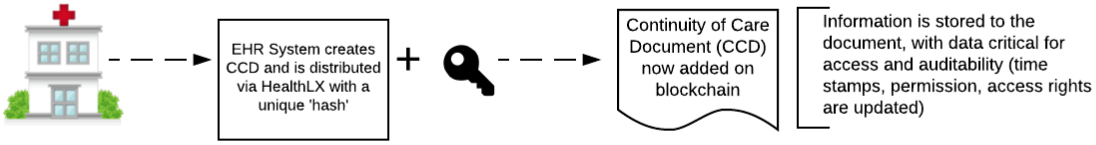
As a result of the above issues alternative means are used to transmit encounter data with phone calls, fax transmissions and the reliance on 3rd party organizations to produce EHR data in a readable format. Depending on the speed to share information ambulatory (urgently) or record-keeping (self-documentation) EHR information is shared without auditability and unique to the nature of the sharing need. Latency and accuracy of data sharing introduces risk to and less-than optimal patient care treatment. To correct these inevitable realities suggests that there should be an approach that addresses each of these critical points. Our proposition is to consider Blockchain combined with CCD digitization for distribution and access to personal healthcare data.

Blockchain leverages existing technology and processes

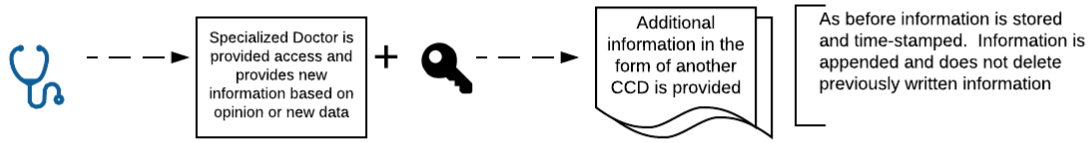
Blockchain eliminates the obstacles described above while also enabling cross-network distribution of patient-approved healthcare data with security and patient-defined privacy. In order to deliver this capability, the verification of the patient through a unique identifier is critical as a point of record consolidation. While the unique patient identifier topic could be debated, and by itself should be a follow-up activity and next steps in the application of blockchain, this topic is not part of this paper. Instead, we will presume that the patient in a medicare / medicaid system is known to be a unique entity. In the US, there are 55.5 million [9] qualified medicare persons so we will presume there exists a unique identifier for these patients. While we are presuming there is proper identification for a patient, there still is a need to associate their patient encounter information (CCDs) across providers to a common means of accessing this disparate data. We realize that this cannot happen overnight but instead becomes a process improvement that does not need to wait. [Exhibit 1]

Exhibit 1

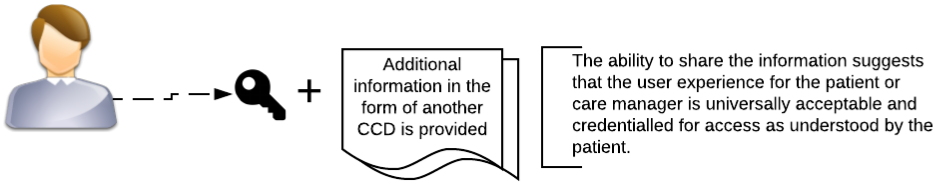
1) Provider(s) records information based on an encounter with patient. The CCD is created with a unique ID



2) Providers, Patient, Care Manager are provided access to blockchain health record



3) Patient or Care Manager(s) are enabled to share or view updated health record to whomever they choose, without regard to where the original data is stored.



Our proposition is that blockchain can be a secure patient credentialing means for record access that leverages currently requested Continuity of Care Documents (CCDs) digitally provided from EHR systems as the authoritative source of truth at the moment in time they were created. Once the CCDs are created, they are made available via blockchain to the patient so as to be properly distributed as the patient or caregiver sees fit.

We submit that our recommendations are not only a pragmatic approach, but also more secure, cost effective and plausible for our current healthcare landscape. Like HIEs, our approach can be instrumental in addressing shared health data, especially in specific segments of the market, such as government sponsored healthcare like Medicare and Veteran Care and other rural care scenarios that have traditionally been supported by HIE models.

This paper focuses on approach and considerations for a prototype to prove the concept. We believe this approach must have some government sponsorship via a sponsored prototype in order to establish momentum and a path towards nation-wide use and acceptance.

Technology Applied; Blockchain and Healthcare

Made popular by Bitcoin, the blockchain technology is known by another name, ‘distributed ledger’. The blockchain technology was made popular by the bitcoin [4] cryptocurrency starting

with the now famous Satoshi paper [5], although there was significant prior work most notably from Nick Szabo [6]. The purpose of the blockchain in context of bitcoin was to provide an "electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." (Satoshi paper [5], "1. Introduction" section)

More accurately, blockchain offers a trust model based on cryptographic proof instead of relying on one (or multiple) trusted parties. This model provides higher non-repudiation characteristics than the model based on trusted parties and was designed to withstand Byzantine attacks [7]. Although our proposal has nothing to do with cryptocurrencies, we believe that the same security requirements like trust in authenticity and integrity of records, authentication and authorization of access to data, privacy, auditability and availability of data make blockchain a suitable candidate for Electronic Health Records via digitized CCDs.

Another key characteristic of blockchain is the reliance on"a peer-to-peer network using proof-of-work to record a public history of transactions that can quickly become computationally impractical for an attacker to change if honest nodes control a majority of CPU power." (Satoshi paper [5], "12. Conclusion" section)

This is a key part of the proposal that addresses the need for:

1. anybody (within the authorization realm) being able to check if a transaction is valid, by means of history being *public*;
2. history is inherently resilient to tampering, by means of many copies being available across a peer-to-peer network.
3. trusted consensus algorithm among peer nodes to agree on what the history is.

Using blockchain in a healthcare system requires one to carefully consider various choices the technology offers. Each of these choices can itself be a recommended approach, however with our approach to accessing healthcare records, there is one implementation that is optimal. Let's quickly review some implementation choices.

Blockchain implementation choices

There are many implementation of blockchain, most notably: Bitcoin, Ethereum, Hyperledger and Ripple. The current proposal does not directly depend on a particular blockchain implementation, but the choice of implementation of the target designed system will have different characteristics. We realize that some implementations are more suitable than others. In the case of blockchain for healthcare, we believe Ethereum to be the best candidate.

Consensus Algorithm

Probably the most important aspect to consider is the choice of the consensus algorithm used by peers to agree on what transactions to include in the history. The Bitcoin blockchain uses a cryptographically strong ‘proof-of-work’ algorithm briefly described in section "4. Proof-of-Work"

of the Satoshi paper [5]. This algorithm relies on some nodes (called 'miners') to solve complex and expensive cryptographic problems. This led to development of algorithms running on Graphic Processing Units (GPUs) or in some cases dedicated high-performance computing hardware. Proof-of-work algorithms were an interesting design choice for financial transactions, allowing anybody to join the bitcoin peer-to-peer network without any trust requirement, again, based on the assumption that one or more nodes with more than 50% of the collective computing power would collude. This design consideration is arguably revolutionary and entirely disruptive to traditional means of recording transactions. In the bitcoin case there is an incentive to have as many nodes joining the network, raising the cost bar for attackers to unsustainable levels. This approach requires the attacker to produce proof-of-work faster than all honest peers combined, which effectively means controlling more than half of the computing power in the network.

That said, we believe the proof-of-work algorithms increases the cost-per-transactions to unsustainable levels and is not a good choice for a healthcare system. There are a number of other consensus algorithms, such as proof-of-stake or proof-of-ownership that we believe provide a similar degree of security and come at a small fraction of the cost.

Our preference for Ethereum as the Blockchain implementation is based on the following assumptions:

- There is a higher degree of trust associated with participants to the healthcare industry (e.g. hospitals) vs the zero trust required by proof-of-work algorithms
- There is little incentive for a participant to the healthcare industry to rewrite history as there are no (financial) gains (except maybe for healthcare liability exposure)
- Fenced in jurisdiction and regulations (such as within a state or a country) further reduce the incentive to attack the system.

The idea behind an algorithm like proof-of-stake [5] (PoS) or proof-of-ownership [6] (PoO) is that only a peer with some proven "stake" is allowed to "vote". We see significant advantages in a system based on PoS or PoO because an external entity (e.g. government) could regulate who could join the peer-to-peer network and have voting power.

Peer-to-peer Network

A key aspect of blockchain technologies, as described above, is the reliance on a public peer-to-peer network that acts as a distributed database of transaction records, aka the public ledger. The technology itself does not put restrictions on who the participants should be. However, in the context of the healthcare industry, we believe that the nodes in the peer-to-peer network that create the blocks (miners) should *only* be trusted stakeholders, such as provider organizations (hospitals).

One key element to consider is the incentive structure. The miners in the peer-to-peer network

do incur some cost associated with maintaining the distributed ledger database. Miners are rewarded for their work via fees "paid" by participants to (healthcare) transactions. Such transactions fees could be agreed upon by the healthcare industry or initially subsidized by the government to incent the innovation. We also believe that the system we propose is economically viable for organizations such as hospitals.

Record Storage

Because new transactions take place every day, there is new data added continuously to the distributed ledger database. Bitcoin for example uses about 500 MB/day of space and about 5 GB/day in bandwidth. This is in a context where the blockchain maintains very little data about a transaction in a block (public keys, hashes and signatures). Because the ledger is distributed on all nodes, it has been demonstrated that storing actual data in the blockchain is not economically practical or even feasible.

We believe this is the only model that scales, but this raises the question of where the actual data resides. We propose the blockchain distributed ledger to be complemented by a secure digital vault service containing encrypted copies of records. Since vaults are not directly related to blockchain, the only correlation being the hashes that also ensure data integrity.

Enablement of existing technologies and the future of health data records

This proposal is for organization and access of personal health records. This healthcare data can be available to the patient or caretaker in similar ways that ‘Personal Health Record’ are used today, but implemented in an entirely different, compelling and cost-effective way. Combining the ideas presented in this paper, we are suggesting that data aggregation via CCDs once accessible from disparate provider systems can be aggregated to the blockchain ledger as an additional data point. Combined with previously received data via digitized CCDs, there exists a timeline of health data history that is maintained on a blockchain data ledger building over the lifetime of the individual. Concepts like attributing other ‘wellness’ data originating from the patient to the Patient Record blockchain ledger provides additional information to be centrally shared with the same level of trust authority.

Over time, access to this information can be used to in numerous ways.

- As evidence of for drug adherence with HealthIT device data collection
- As evidence of care plan management, patient performance and outcomes
- Vital statistics can be shared with multiple unrelated parties at the patient’s choosing such as caretakers, insurers, family members, or self-wellness.
- This data could be used by healthcare programs to assess the health of the person whose data is contained at the patient record for evidenced-based care.

Currently, medical records are stored and maintained by each entity participating to the healthcare system via a software application called an EHR system. There is no uniformity in the way EHR systems are maintained and operated and the level of risk and exposure to

attacks is dependent on the skills of the organization hosting the EHR application. As demonstrated by many cyber attacks in the past years, most famously the attack on Anthem, February 4, 2015. In this example, attackers had broad access to medical records. For small clinics and solo providers who do not have both the budgets and the skills, the burden of maintaining electronic medical record integrity is unreasonably high such as in rural areas. We propose a system of maintaining electronic medical records that addresses the challenges above and complements the established EHR systems. The key elements of our proposal are :

Assumptions concerning CCD access, content and creation

- All records are kept in their original form using an established standard, e.g. CCD, digitally available by request from an authenticated requesting agent
- All CCDs are hashed; hashes have dual purpose, both as document identifier and integrity check.
- All CCDs are transferred and stored in an encrypted form within blockchain
- CCDs may contain references to other CCDs or data (such as Patient ID in an MPI - Master Patient Index); as such an MPI could be completely anonymized
- CCDs are stored by a Custodian equipped to properly operate a Digital Vault.
- A Custodian stores encrypted CCDs along with their hash signed with the Custodian's (Digital Vault) private key.
- CCDs are stored by more than one Custodian to provide redundancy and prevent data loss
- All transactions, including creation and transfer of CCDs are recorded in a blockchain
- Blockchain is maintained by a network of peers (we'll keep using the established Miner term)
- An entity could be both a Miner and a Custodian

Benefits to the Healthcare Industry

- Stored centralized CCD establish a health data history over the life of the individual but do not store identifying information about the individual.
- The record of which CCDs belong to who is separated from the CCDs that are centrally stored, and hashed. They do not include full patient identifiable information which makes a data breach less valuable because the difficulty of tying the records to the individuals.
- Transfers of the CCDs would be encrypted to help suppress the theft of data by listening and the records do not have patient identifiable data. The record request would be for a record number associated with a patient so the patient identifiable information would not be transmitted across the wire in the same conversation.
- Data breach at a custodian would yield encrypted records that are not associated directly with patients but only contain record numbers as the identifying record making the data theft of minimal value.

- All transactions are recorded in the blockchain transaction history ensuring honest account of who accessed or changed records and gives a history that is able to be recreated if there is suspicion of unauthorized access. Altering the history of access would be prohibitively expensive increasing in cost as adoption grows.

Incorporation of Open Source

This proposal, like the healthcare industry in general, relies upon multiple parties with different roles. For that reason we believe that the best way to implement the solution we've proposes is as an open source project.

Open source technologies have wide acceptance in the industry nowadays. It is common for successful large projects to be developed as open source with multiple vendors providing commercial distributions and support. There are countless examples, from the Linux operating system variants to Apache Software Foundation (ASF) projects. Blockchain technologies we intend to build are on top of other development efforts originating as open source projects themselves (including Bitcoin, Ethereum or the Linux Foundation Hyperledger project).

The main difference between commercial and open source projects is that the latter rely on a strong communities to thrive. Open source communities provide the forum for multiple stakeholders with a vested interest in voicing their needs and cooperating on the roadmap. Community contributions to these ideas are crucial for engagement, acceptance and broad adoption.

Our team includes of open source committers and contributors with broad experience and proven track record in building successful, widely adopted open source projects, mainly at the ASF. Our experience is not only in developing high quality software, but also as community builders and mentors of incubating projects and speakers at open source conferences in the US and abroad. We have contributions across the healthcare interoperability domain, where we have leveraged existing standards such as HL7, FHIR, and the open-source projects like Apache Camel, ActiveMQ, CXF, Karaf and VA's VistA (OSEHRA)

Conclusion

In conclusion, we are introducing our blockchain idea as a means to 'flip the office' as was proposed at the 2016 ONC Annual meeting. We believe Blockchain is an evolutionary approach to enable trust unlike any other technologies previously considered. We believe our approach to implement blockchain is essential to supporting the ONC's interoperability roadmap and crucial to the long-term fabric of a learning health system. With a means to address 'Trust' across patients, payers and providers our national healthcare direction can achieve the objectives in the ONC roadmap and meet future generations' healthcare needs. Accepting this approach is no small challenge but the reward is too great to ignore.

References

[1] ONC Interoperability Roadmap V 1.0, page 12
https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf
[2] “Pledge” https://www.healthit.gov/commitment
[3] Center for Medicare and Medicaid Services [CMS-5517-P] Section 106(b)(2)(A) of the MACRA amended section 1848(o)(2)(A)(ii) of the Act.
https://s3.amazonaws.com/public-inspection.federalregister.gov/2016-10032.pdf
[4]: https://bitcoin.org/en/ "Bitcoin"
[5]: https://bitcoin.org/bitcoin.pdf "Satoshi Nakamoto paper: Bitcoin: A Peer-to-Peer Electronic Cash System"
[6]: https://en.wikipedia.org/wiki/Nick_Szabo "wikipedia: Nick Szabo"
[7]: https://en.wikipedia.org/wiki/Byzantine_fault_tolerance "wikipedia: Byzantine fault tolerance"
[8]: https://en.bitcoin.it/wiki/Proof_of_Stake "Proof of Stake"
[9]: “Kaiser Permanente Medicare Beneficiaries 2015”
http://kff.org/medicare/state-indicator/total-medicare-beneficiaries/