CA Gov Ops Blockchain Working Group
HEALTH RECORDS
By Radhika Iyengar and Arshad Noor
March 27, 2020

Introduction

Health records are at the heart of healthcare. It is widely accepted that in order to achieve the best health outcomes, we must have good quality records that capture a complete medical and health record and contiguous context for a person's health. This leads to a successful collaboration between a patient and any physician or health professional. It also fosters a tailored and personalized care approach, which bolsters high patient engagement and patient empowerment. This value-driven approach is the one that all healthcare stakeholders are striving for, and all patients need and seek, yet the reality is far from it.

With healthcare data fragmented across the spectrum, there is currently a spotty, or episodic context at best, for a person's health. EHRs (electronic health records) were conceived as the means to weave a more complete health context for patients, and today in the US, we have high adoption of EHRs, yet the promise of EHRs has not been realized. Health data remains siloed and has not achieved the degree of interoperability needed to bring disparate health data sets together to deliver a unified health context around patients. There are different types of EHRs, and despite moves to create unifying standards such as FHIR (Fast Healthcare Interoperability Resources), these standards have yet to mature further and overcome other inherent inconsistencies around interoperability to deploy across health systems. Thus, EHRs have not been able to achieve the outcomes for which they were created.

Added to the EHR challenges, it is important to point out that current financial and administrative structures do not incentivize patient-centric care. Fee-for-service models are still predominant, and experts agree that this transactional approach prioritizes volume of visits rather than quality of care. Current financial and insurance frameworks further incentivize fee-for-service models, by prioritizing those that can afford healthcare. It is well documented that current reimbursement models are ineffective. In California, doctors struggle with getting reimbursement for MediCal patients, so it disincentivizes doctors from accepting MediCal. This undermines health accessibility and does not permit the people who often need healthcare the most from receiving healthcare. It also drives up the incidence of ER visits which further exacerbates the cost of healthcare.[1]

From a health data perspective, the patient or healthcare consumer continues to remain at the fringe of the data continuum, with limited control and less empowerment in their own health journeys. Today's centralized health data systems further silo the data. Limited data sharing means that it is very difficult to construct a complete and contiguous health record for an individual. Additionally, prevailing poor security protocols around health data attract aggressive cyberthreats and leave data stores increasingly vulnerable to crippling data breaches like ransomware and high financial loss. The construct of current health data

stores places the burden of providing adequate defense to cyberthreats on providers, payers or other entities which keep copies of health records. Healthcare CIOs have broadly declared security to be one of the most difficult and financially devastating issues in healthcare.

Finally, let's examine the ownership of data, inherent to the above discussion. Patients by law might have access to their own data, but they do not have their whole health record. Health providers argue that they do not own the data, and that it is the patient's responsibility to keep their records unified. Even those health systems that provide a complete record to patient members can only offer this in a limited manner. If a patient needs to seek medical services outside that health system, data sharing is painful, time consuming, and often incomplete. Clearly, the patient bears the burden of trying to establish a continuous and cohesive health record, painstakingly requesting copies of fragmented health records and finding a way to keep these records together, easily accessible and secure. From a health identity perspective, individuals have no true ownership or control over health data.

Context for California

At 39.5 million residents, California is one of the most populous states in the US. From an innovation and policy perspective, what California does is thought to be meaningful at the national and global stage as CA's vision can often influence the broader discussion on innovation and policy. From a budget perspective, there is an imperative to improve processes and regulations in California to achieve better health outcomes. California's 2019-2020 budget is just over $209 billion, of which just over $40 billion or just over 19%, yet this significant investment does not correlate to desired health outcomes for California residents. Healthcare has a broad umbrella of issues ranging from financial/administrative, policy and regulatory compliance, health recordkeeping, health data storage and access and associated issues of identity, security, privacy and interoperability.

From an insurance and corporate practice perspective, the Mercatus Center at George Mason University ranks California 40th out of the 50 states in healthcare accessibility, and emergency room visits have increased by 10% since Obamacare. The Mercatus Center research further points out that CA "inhibits the development of innovative business models that could potentially lower the cost and improve the quality of care". Examples include innovative delivery models such as direct primary care (DPC) in which "a primary care doctor charges patients a retainer fee covering all or most primary care services, including clinical, laboratory, and consulting services … A DPC practice charges periodic fees for services, generally $25 to $85 per month, … DPC practices claim to reduce administrative overhead by approximately 40 percent." The DPC model is gaining popularity in other states such as Hawaii, Utah and Wyoming, and is being recognized as an approach to move away from the fee-for-service model. California currently does not support the DPC model.[2]

From a state policy perspective, there are measures that demonstrate California's forward-looking position, for example CA's stance on OTC oral contraceptives. CA is positioned to extend its leadership the way in progressive thinking in the delivery of healthcare. The treatment of health records can be an area in which California can open up to more modern and forward-looking frameworks that serve CA residents more impactfully and more completely.

Health recordkeeping is yet another issue. With the goal of establishing complete, contiguous records, there is a need for relevant records throughout a lifetime. California law requires hospitals to keep a patient's records for up to 7 years. MediCal requires that records be kept for 10 years. These recordkeeping requirements might seem long enough but are not adequate as patients need to manage their health records across multiple providers across their lifetimes. What is importantly missing is portability as people move from one place to another, and frequently across providers or payer systems. Modern health contexts are dynamic models, so patients need to have their records portable, private and persistent - accessible anywhere at any time and shareable with health professionals or other entities of choice. Current data storage and sharing models are ineffective and inadequate at being able to provide ubiquitous access to health records.

Interoperability and administrative burdens are other important issues not only relevant to California but also nationwide. In fact, the California Hospitals Association (CHA) responded to a draft letter dated January 2019 from the Department for Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) and Centers for Medicare and Medicaid Services (CMS) urging them to further reduce burdens of Health IT and EHR to enable doctors to focus on giving more quality time to their patients. They request "greater detail to be provided around clinical documentation, EHR and electronic clinical quality measure (eCQM) reporting and public health reporting." The CHS also requests the ONC to "articulate in greater detail specific methods that will reduce the barriers to interoperable exchange of health information in order to accelerate its adoption nationally."[3]

Current clinical documentation processes are not "updated to take into account the integration of HIT systems, greater clinical complexity of patients and available treatment options or the increased need for longitudinal, coordinated care." [4] Present IT infrastructure is mixed in maturity – EHRs are pervasive but data capture and systems can be archaic and paper-based. From a staffing perspective, there is a need for blockchain-trained professionals. LinkedIn has stated that blockchain expertise is the number one most sought after hard skill. The technology is still developing, but there is exponential growth already visible in this expertise.

Interoperability between systems remains challenging despite data standards. The CHA points out that interoperability should be a bigger focus of the draft letter from the ONC and that this focus is "notably absent." The CHA declares that "despite extensive efforts by our state, we are still plagued by disparate health information exchange efforts that are not well coordinated." Clearly, the CHA response is a cry for help for greater clarity, definition

and prescription to move forward and accelerate the adoption of interoperable digital health records.

Interoperability (Adapted from the book *Enterprise Blockchain Has Arrived* by Radhika Iyengar and Jorden Woods)

Currently, ready access to comprehensive patient data through EHR systems has been riddled with problems: patient data is fragmented across too many healthcare stakeholders and different providers invariably use different EHR systems. We have even heard of health systems that have different flavors of EHR systems among many internal divisions making interoperability within a health system difficult, let alone across a health ecosystem. Interoperability challenges silo the data so that it stays where it was collected. Struggles with interoperability spawn other issues around health data. Today, in order to improve data interoperability and cross-system engagement, as well as patient engagement and clinical support, the healthcare industry largely uses technology connected to the Internet. This practice, combined with poor security protocols at many healthcare facilities, have made centralized EHR systems easy targets for hackers who have stolen millions of patient records or created chaos with cyberthreats such as ransomware attacks. A cyberthreat is a major cyberattack that has seriously damaging implications. Ransomware renders a provider completely shut out of necessary information and tools that are being used in either diagnosis, management or treatment. The 2017 Wannacry attack is infamous in illustrating the severe extent of damage that ransomware can cause.

In 2018, one of the large health systems suffered 87 billion cyberthreats. Although this figure is on the exceptionally large side, other organizations can have billions of cyberthreats. In many cases the threats remain unknown for many months. Due to these types of critical security breaches, many healthcare facilities have become wary of sharing or transferring data from EHRs for fear of further breaches, unwelcome negative media attention, and loss of community trust.

Since patient data is stored with multiple stakeholders and fragmented across disparate systems that are not easily interoperable, it is not easily shareable as a comprehensive historical record. For example, cancer patients may have their CAT scans stored at different labs, radiology notes located with various radiologists, their chemotherapy records at a number of hospitals, other visits and notes (in disparate electronic formats) with various other providers, medication records with pharmacies, medication adherence records with other companies, etc. Any potential solution must therefore work well in a distributed ecosystem as well as improve trust and interoperability between different stakeholders.

Blockchain technology has tremendous potential in healthcare and particularly for healthcare data. With the right access to patient-owned healthcare data, health systems can offer optimized care to patients, from providing personalized, predictive diagnosis and treatment, to precision medicine and preventive care. Blockchain also provides a valuable benefit in making the healthcare journey more participatory.

With data ownership individuals can share their health data with healthcare providers in a secure, private and selective manner, anytime and anywhere. It is the individual will be at the

center of the health journey and empowered to engage and participate. From a provider's perspective, high personal engagement and participation means that the healthcare process becomes a collaborative approach, likely to result in significantly better health outcomes delivered more efficiently.

Without adequate and well-defined frameworks to reduce critical data interoperability barriers, streamlined clinical documentation or increased quality measures, health systems for California, and more broadly in the US, will continue to struggle in delivering the high quality of health care being sought. Blockchain technology has the capabilities to solve many of these systemic issues from seamless, realtime coordination and integration of complete and contextual health data across disparate health systems.

Due to regulatory constraints it may not be possible to fully decentralize the healthcare system with blockchain. Instead, trusted ecosystem players such as hospitals, insurance companies, clinics, labs and health information exchanges (HIEs) may become part of the processing fabric of the system since they can still store and process patient data. With blockchain, there will be significantly improved data sharing and interoperability, which will result in better patient data management and coordination on the backend. From a patient perspective, this improved backend coordination will provide a better point of care experience.

An example of this implementation is the collaboration between blockchain startup Burst IQ, the data analytics company Empiric Health, and Intermountain, a Utah-based not-for-profit health system comprising 22 hospitals, 1600 physicians and 180 clinics. Burst IQ uses blockchain, advanced security big data and machine intelligence to provide a health data network that manages, stores and analyzes health data. The system also offers data sovereignty and privacy to enable a diverse stakeholder ecosystem including patients to collaborate around health data. Intermountain is utilizing Burst IQ's blockchain platform and Empiric Health's machine learning platform to bring about increased efficiencies and significant cost reductions in their surgery practice. Since 2017, millions of dollars in cost reductions have been achieved.

Who benefits from improved data collection, storage and workflow?

The short answer is all stakeholders, including government entities, patients, providers, and payers, stand to benefit from improved data collection, storage and workflow. Data storage is particularly important for compliance with retention of healthcare records. Currently providers and payers are responsible for storing and managing confidential health records. Decentralized data storage with hashes of health records stored on the blockchain will provide verification of data authenticity and integrity. Further, with data sovereignty patients will take ownership and control of their health records and can safeguard the privacy of their records with selective disclosure mechanisms. It is important to note that some of the responsibility and burden of managing health records is thereby transferred to patients.

Parameters for Consideration Regarding Security and Privacy

HIPAA is a requirement for privacy in health records. Providers and payers must preserve privacy, but patients are by law permitted to have access to their own records. Security is also a requirement for protecting health records as well as safeguarding privacy, but current security protocols are not effective at preventing cyberthreats like ransomware. We have discussed previously how the interoperability challenges have led many providers to solve these issues relying on Internet connectivity, further leading to security risks and breaches. We have also discussed the relationship between identity and privacy – both are intertwined with patient records, but patients still have no ownership or control over their own complete records. For a more in-depth discussion on privacy, refer to the Privacy considerations and Digital Identity sections of the CA GovOps Blockchain Working Group.

Of all the opportunities for blockchain in healthcare, there is the creation of the Personal Health Record (PHR) which goes far beyond the EHR. The following is an excerpt of the book, *Enterprise Blockchain Has Arrived*.

Blockchain technology can make secure PHRs a reality. It is a key building block of the ecosystem because it will contain a patient's fully self-sovereign and private record of medical history, and will include treatment history from providers, patient-generated health data, and a summary of patient health information, including:

- Personal identification
- Vitals
- Family medical history
- Medical conditions
- Medications
- Allergies
- Immunizations
- Diet restrictions
- Microbiome data
- Genomic data

A PHR enables each person to own his or her own comprehensive personal health information and share this data across the ecosystem to receive optimized care. To date, PHRs have not gained widespread adoption because of significant security and identity concerns. However, blockchain technology paired with SSI and DID makes it possible to achieve a true PHR by simultaneously addressing these concerns in a single system.

Mass adoption will also be possible if users can embrace blockchain-based healthcare dApps (decentralized Apps) and smart contracts on mobile devices worldwide. Once PHRs achieve widespread adoption, there is still a concern regarding the implementation of PHRs — particularly the unauthorized copying, sharing and storage of healthcare data during transmission, arguably when data is most vulnerable. As we discussed above, hackers are persistently attacking health data repositories to get access to medical records, especially identity information. Additionally, there are high security authentication mechanisms via biometric and multi-factor authentication that are critically important.

Since healthcare providers will need to be able to read patient information for optimizing care, other cryptographic techniques and approaches will be required to ensure that the data cannot be copied, transmitted, or stored at any time. Each person can provide selective disclosure of critical historical personal information to authorized healthcare providers and other ecosystem players to minimize the potential for unauthorized access.

Finally, privacy mechanisms such as zero-knowledge proof (ZKP) can enable selective disclosure ensuring that only required information changes hands during any transaction. As a result, individuals will be able to restrict the flow of sensitive information and place conditions, such as expiry date, on data that is shared. To comply with regulations (i.e. HIPAA), each PHR should be fully self-sovereign, or owned by the individual, since the data is rightfully theirs. With self-sovereign identity (SSI) and decentralized identifiers (DID), combined with high security biometric or multi-factor authentication, it will be possible to unlock your PHR in your digital wallet. Trust is intermediated by technology-based rather than people-based verification mechanisms. With SSI and DID, the PHR can become that portable, persistent, and private health record available to us anywhere, anytime.

Most solutions envision that each person controls the level of access to the data and can even charge for access via blockchain technology's smart contracts. In fact, it is the SSI concept that underpins the ability to control access to your data. A key idea in the blockchain community is that individuals should be able to control and monetize any information connected to their digital identities. Some of the more effective blockchain-based PHR solutions ensure that each PHR has a unique digital address, that data is fully encrypted and cryptographically signed, and that it is interoperable with common EHR systems.

Overall, blockchain-based PHRs have the potential to improve healthcare outcomes and reduce costs by increasing speed and efficiency in the management of health data. They can also accelerate the transition to patient-centric healthcare by putting the patient and the patient's data at the center of the healthcare ecosystem.

An example of an early deployment in this area is the Health Blockchain Consortium from US/France-based Embleema. Embleema was founded on the premise of providing patient data sovereignty to improve health outcomes. In 2018 they launched their beta platform and established the Blockchain Health Consortium with Servier, a French global pharma company. The consortium pilot brings together an ecosystem of patients, providers, pharma, and clinical research. The consortium is focused on enabling patients to share their digital health data real-time with the aim of improving patient engagement. For the consortium, Embleema has also partnered with Cystic Fibrosis, Pierre Fabre Médicament, IEEE and Hyperledger.

What are the trade-offs with blockchain? What are the potential risks and benefits?

When developing the healthcare framework for California, we can look at other ecosystems, even globally, to have a base of reference. Consider the healthcare models of Dubai or Estonia, both progressive ecosystems that are considering or have deployed country-wide deployments of DLT-based health systems. As we move forward through this process, we need to roadmap

for success so that we are able to demonstrate value in the blockchain implementations the state will pursue.

1. Prioritize problems to focus on for which blockchain has a useful application and solution
2. Define the use cases that will be pursued
3. Define concrete, near term pilots/POCs/Sandbox, bringing together allies, partners both in industry and tech – depending on the pilot/POC/Sandbox, consider whether you will make this implementation more permissive from a legal perspective (e.g. lower tax rate for blockchain networks)
4. Agree on standards and best practices in the implementations
5. Demonstrate success in these use cases
6. Determine what next steps ensue after success is established through pilots and POCs
7. Re-align with allies and partners, and identify new partners, both industry and tech
8. See if you can interoperate with other chains
9. Repeat process to take implementation further and amplify adoption

With any system, a feasibility evaluation begins with scenario analysis – from remaining with the status quo to on-ramping with blockchain. There must be a thoughtful approach starting with a problem and evaluating what makes sense in solving a problem. Clearly the status quo is untenable – that is the biggest risk as existing systems are inadequate from the perspective of patient identity, adequate privacy and security, and data interoperability. There are other technology risks in blockchain including scalability, governance, potential cross-chain interoperability as well as blockchain-to-legacy system challenges. Permissioned systems are currently better positioned to deliver solutions that effectively address these challenges but deployment across a large state such as California will need to take scalability to high level. There are other technology challenges such as large scale private key management across the California population.

Before embarking on blockchain-based systems, discussion with patient advocacy groups, health consortia, health systems, hospital CIOs, executives at payers, and blockchain for healthcare platforms will help in understanding the viewpoints of all stakeholders and technical considerations of all stakeholders. We must also consult with healthcare government agencies and entities including The California Health & Human Services, California School Districts and organizations that need to review immunization records, Center for Disease Control, Immigration & Customs Enforcement (passengers detected with communicable viruses), Food and Agriculture (dangerous bacteria detected in the food supply chain resulting in emergency healthcare), etc. Here again, blockchain is a community driven ethos, and blockchain-based frameworks address ecosystem spanning collaboration. From this standpoint alone, there is a valid reason to fully evaluate the feasibility and deployment of blockchain-based health systems in California.

Conclusion

We are at a point in time in which current health systems are so rife with challenges of data fragmentation and silos, lack of cohesive patient identity and privacy, and pervasive security challenges that it is unthinkable to remain with the status quo. With all the rhetoric of value-based care, healthcare continues to remain a volume-based, one-size-fits-all model. Until a framework for providing patient identity is adopted pervasively, there will be continued attacks on centralized health systems and data 'honey pots.' Until robust data interoperability is achieved, cohesive data context for patient records will remain elusive as will the goal of achieving true value-based care.

We have an opportunity to construct a health system for California that moves us into a modern, personalized healthcare system that can largely be achieved with the adoption of blockchain-based systems, combined with other advanced technologies such as AI/ML and IoT as appropriate. With this convergence of technologies, we can finally put the individual at the center of the care continuum, with control over a complete health record that is selectively shared with healthcare providers to improve the outcomes and care along our health journeys.

Recommendation

This section, yet to be defined, will be in the form of the high-level specification of a pilot CA project to explore the use blockchain in healthcare records. As an initial use case, Arshad Noor and Radhika Iyengar have been considering CA's immunization records. These records involve CA government, healthcare organizations, providers, patients, school districts and schools.

Arshad and Radhika have been in touch with the CA Immunization Registry to understand the system that currently exists in CA. They will be having a series of discussions with CAIR and other entities before making a recommendation to test blockchain for immunization records in CA.

Bibiliography

Note: Major portions of this report have been adapted from the book, *Enterprise Blockchain Has Arrived*, by Radhika Iyengar and Jorden Woods, copyright May 2019.

Additional general resource: https://www.healthit.gov/sites/default/files/page/2018-11/Draft%20Strategy%20on%20Reducing%20Regulatory%20and%20Administrative%20Burden%20Relating.pdf

1. https://www.forbes.com/sites/sallypipes/2018/07/23/californias-costly-inaccessible-healthcare-system/#62689aea32f6
2. https://www.mercatus.org/system/files/bryan-healthcare-hoap-apr2019-mercatus-project-overview-v1.pdf
3. https://www.calhospital.org/sites/main/files/file-attachments/cha_comments_onc_draft_strategy_to_reduce_ehr_burden_012519_final.pdf
4. https://www.mercatus.org/system/files/bryan-healthcare-hoap-apr2019-mercatus-project-overview-v1.pdf