Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.

8283 Greensboro Drive
McLean, VA 22102

www.boozallen.com

August 8, 2016

Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
200 Independence Ave SW
Washington, DC 20201

Attention: Debbie Bucci
Reference: "Blockchain and Its Emerging Role in Healthcare and Health-related Research" Ideation Challenge

Dear Ms. Bucci:

Booz Allen Hamilton, Inc. (Booz Allen), in partnership with Microsoft and ConsenSys, is pleased to submit our white paper to the Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology. This white paper is in response to the Ideation Challenge solicitation of white papers on the topic of Blockchain Technology and the potential use for Healthcare, published on July 8, 2016 on the Capital Consulting Corporation's Innovation Center website.

Booz Allen looks forward to the opportunity to engage further with HHS on blockchain innovations. For any questions you may have or continued discussions, please contact Victoria Adams at (703) 507-6911, by email at Adams_Victoria@bah.com

Sincerely,

Kathryn Kienast
Principal
BOOZ ALLEN HAMILTON INC.

1 INTRODUCTION

Booz Allen Hamilton, ConsenSys and Microsoft are pleased to submit this white paper to the Department of Health and Human Services for the "Blockchain and Its Emerging Role in Healthcare and Health-related Research" challenge on the topic of Blockchain Technology and the potential use for Healthcare.

Blockchains are one of the most significant technologies to emerge since the Internet. By providing decentralized, cryptographically secure, transparent, and auditable methods of exchanging information, blockchains offer the possibility of disintermediating a range of industries, including healthcare. In particular, blockchains have been identified as able to enable or facilitate solutions to a number of significant industry concerns including (but not limited to): (1) encouraging secure exchange of healthcare records and secure communication between healthcare providers using time-stamped, controlled access electronic health records; (2) identifying and guarding against fraud in claims submission while; (3) reducing processing cycle time for initial claims and decreasing the volume of appeals; and, (4) improving inventory management and drug and medicine tracking. These solutions have the potential to frame significant quality and cost improvements throughout the entire healthcare ecosystem. In this White Paper, we describe how blockchain technology can be leveraged to achieve these results and discuss the possibilities for its potential use in Health IT to address privacy, security, and scalability challenges of managing electronic health records and resources towards these goals.

The firms collaborating on this submission each bring top flight expertise and experience in Health IT and innovative solutions and ideas:

Booz | Allen | Hamilton Booz Allen Hamilton is one of the largest public sector management consulting firms offering strategic planning, IT, healthcare, and technical assistance capabilities. Our team of 2000 healthcare professionals covers a wide variety of healthcare expertise, including health policy, program integrity, health insurance and payment, grant management, regulatory science, Health Information Exchanges, pharmacy benefits management, chronic disease management, and health care delivery. Booz Allen brings specific experience supporting CMS with the implementation of new programs such as Medicare Part D and the Marketplaces created under ACA, as well as with conducting significant health plan evaluation activities. In addition, Booz Allen is a leader in the development of blockchain technology within the Federal government. Over the last year, we have invested heavily in developing use cases and technology applications for blockchains within the public sector and have worked with a number of agencies (e.g., FDIC, CFPB) to explore how blockchains can be used within the Federal government.

Microsoft Microsoft has made deep investments in blockchain and has developed Blockchain as a Service (BaaS), which provides a rapid, low-cost, low-risk, and fail-fast platform for organizations to collaborate together by experimenting with new business processes—backed by a cloud platform with the largest compliance portfolio in the industry.

CONSENSYS ConsenSys is a venture production studio that specializes in building decentralized applications (DApps), enterprise solutions and developer tools for blockchain ecosystems, focused primarily on Ethereum. Powered by smart contracts, and secured through encryption, ConsenSys' applications provide the benefits of transparency, auditability, and immutability that are unique to blockchain-based solutions.

2 BLOCKCHAIN'S VALUE TO HEALTHCARE

As expressed in the Shared Nationwide Interoperability Roadmap from the Office of the National Coordinator for Health Information Technology, we must maximize information sharing among all participants in healthcare – patients, providers and institutions - to streamline and improve healthcare

services and implement fully value-based payment policies that incentivize collaborative patient-centered outcomes, research, and precision medicine. Booz Allen, ConsenSys, and Microsoft propose a decentralized, secure, vendor-neutral solution that supports the easy implementation of modular, blockchain-based health records, while maintaining the existing Health IT infrastructure. Blockchain technology has the capacity to expand and allocate trust from the current state of one-to-one contracts and data use agreements to the broadly available yet secure history recorded in the blockchain computation, enabling the many stakeholders who impact the health of an individual to communicate and collaborate securely, efficiently, and democratically. Integrating blockchain into Health IT will:

- **improve the interoperability of existing networks in support of value-based care**
- **create a foundation for patients to take ownership of their healthcare, while empowering them to be educated decision makers.**

3 DESCRIPTION OF TECHNOLOGY

Blockchains are a form of distributed ledgers, originally proven viable by Satoshi Nakamoto's now familiar Bitcoin blockchain. The Bitcoin blockchain was a transaction history (ledger) formed and legitimized by every stakeholder in the Bitcoin network through distributed consensus. Because a ledger naturally accompanies monetary transactions, it is easy to recognize Bitcoin's use case for the blockchain. However, by understanding that Bitcoin and all other forms of money are simply representations of value, blockchains emerge as the accountants for anything that has value--including identity, authorization, and electronic health information. The blockchain is an instrument that enables mutually untrusting organizations to work together in highly competitive markets by replacing the procedural inefficiencies of interparty transactions with transparent and authenticated interactions conducted on shared infrastructure.

Although blockchains seem like nascent technology, they are actually a combination of proven, trusted technologies. Blockchains compound databases, networks, and cryptographic security. Encryption secures the transmission of data across a network by ensuring that the intended parties (the senders and receivers) are the only members of the network capable of reading data. There are two types of encryption that every modern web browser employs today: symmetric key encryption and asymmetric key encryption. In symmetric key encryption, only one private key encrypts and decrypts data. In asymmetric key encryption, a pair of keys--one public and one private--encrypt and decrypt data, respectively. Encryption standards that have resisted attacks for two decades are the backbone of identity verification on the blockchain and can protect electronic health records as patients selectively disclose information to their healthcare providers. Public key cryptography provides the native access control protocol on blockchains. A user's identity is defined by a public-private key pair in which the public key asserts an identity and the private key proves the identity. Unlike in traditional databases through which access control is managed by separate software running a layer above the database, programmable blockchains allow access control to be defined in a way that is inherent to the data being stored.

Blockchain technology, the means of consensus, and the classes of problems over which consensus may be formed have all been expanded and improved hugely since the advent of Bitcoin in 2008. Programmable blockchains allow for *trusted*, *auditable* execution of complex business processes between and within organizations. This is accomplished by combining a uniform application layer with a shared database. What is special about blockchains relative to other databases is that they achieve fault-proofness or authenticity by enabling their state to be mathematically tested for consistency over time by any party which is a "participant" in the blockchain, and these participants need not trust one another. The Ethereum

blockchain, for example, is a fully-programmable blockchain with a Turing-complete virtual machine that can execute peer-to-peer applications called smart contracts.

Furthermore, programmable blockchains do not distinguish between data and code. This means that applications in execution, when run on blockchains, are subject to the same mathematical fault-proofness as the data they operate on. Smart contracts can store data and trigger cascades of other interactions that are independently defined and outside the scope of the original transaction destination. Therefore, using smart contracts, blockchains enable businesses to function as public APIs in which the businesses' identities and digital signatures are defined by a public-private key pair.

Prior to the advent of blockchains, business logic had been implemented as an access layer atop a process agnostic database. This is a large part of the reason database access is so controlled: access without the officially sanctioned means can effectively corrupt the database by breaking the assumptions of the business logic. It is unsafe to access a database without the mediation of business process software. By using a blockchain, the database and its business logic are made intrinsic to one another; the database is natively defined by the business logic, from which it cannot be separated. Because interactions with the data are permissioned by default according to the business logic, the interaction interface can be opened to the world. This enables the general public to initiate transactions with a medical record and safely rely on code instead of a third party to ensure privacy and security. If a set of transactions are particularly sensitive and only intended for certain parties, an on-chain access control gate can make transactions viewable only to those parties. This protects mental health and other highly sensitive information from being shared when unnecessary.

The solution we propose makes use of a programmable blockchain, Ethereum, and a decentralized file system, IPFS. In addition to familiar encryption technology, our solution also makes use of hashing algorithms which are used to generate a unique fingerprint for data. Just like the impression of a fingerprint, which reveals no information about the individual from whom it originates in spite of being unique to them, it is impossible to use a hash to learn anything about the underlying data from which the given hash was produced. We will use IPFS to store encrypted data, and the hashes of the data are stored in a smart contract on the Ethereum blockchain.

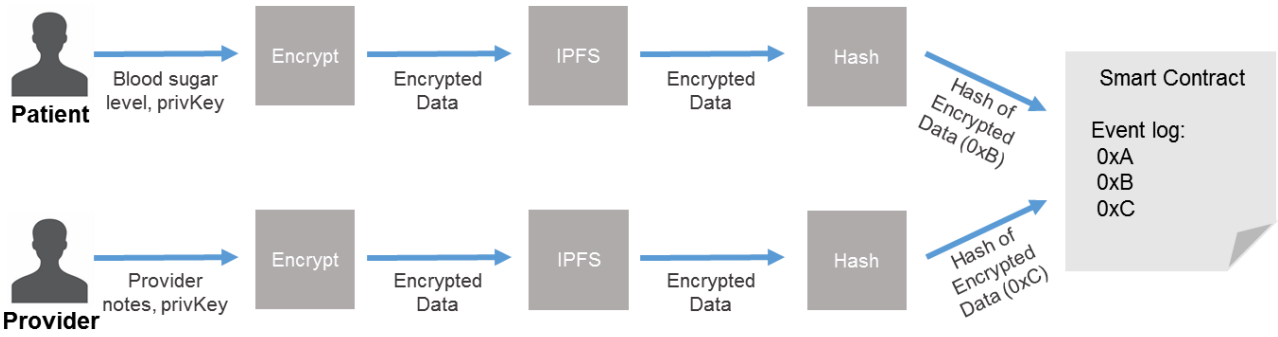
4 USES IN HEALTH IT AND/OR HEALTHCARE RELATED RESEARCH FOR TECHNOLOGY

Blockchains may be catalysts for change in the fragmented United States Healthcare System by enabling direct, transparent, authenticated interactions between patients and the multitude of individuals impacting their health. Currently, health information in electronic form resides in numerous locations, but principally in Electronic Health Records (EHRs), medical devices, Personal Health Records (PHRs), patient facing mobile apps, and survey instruments. EHR software providers, provider networks, and PHR repositories operate in an environment that is not yet designed to effectively interoperate, educate consumers, or optimize many healthcare processes. Patients still have difficulty accessing integral information about their healthcare services, and their multiple providers may not be able to communicate to generate a holistic view of the patient to provide precise care.

Electronic health information will remain fragmented and incomplete while there exists a repeated need for the patient to repeatedly establish and reestablish his/her identity and medical history across multiple care providers, which is cumbersome and contrary to the conveniences that electronic health information should enable.

Blockchains make all stakeholders equal citizens in an inherently transparent, decentralized infrastructure that obviates the expensive process of connecting data silos by providing an open trust framework for all participants to reliably interact in. Our proposed solution builds on the technology and investments made to date, equips providers with the ability to seamlessly and securely access and use health information from different sources, and empowers patients to own and control their health information in a way that puts them at the center of their care. The result is a longitudinal health record that all stakeholders can contribute to and learn from while maintaining the privacy of the patient. The system also allows patients to selectively disclose information, whether for specific providers or for public health agencies and researchers to use in developing patient-specific treatments. Blockchains provide a framework to exchange and use electronic health information between multiple systems with reduced effort on the part of the users.

Architecture:



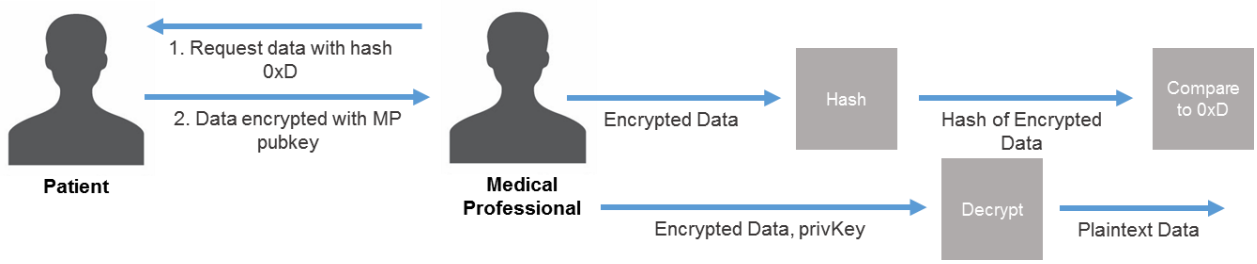
A single patient has many healthcare providers that each have an EHR/EMR for that patient. It is very burdensome for the patient to access and analyze his/her complete medical history given the current state of interoperability. Patients should be able to store their verified medical history in one place and selectively share parts of that information with whomever they choose (healthcare providers, pharmacists, researchers, etc.) to develop a more holistic understanding of their health.

Booz Allen, ConsenSys, and Microsoft propose an open EHR protocol and infrastructure that is sufficiently interoperable with existing EHR software such that those systems can read and write data compliant with the protocol while continuing to serve data in the view layer in whichever manner customers are used to. The protocol allows patient-specific electronic health information recorded on any EHR software by any healthcare provider to be securely and automatically transcribed to a patient-owned record on a public blockchain. By using public computing infrastructure like a blockchain, patients can own their complete medical history, to which all of their care providers contribute, and which the patient can selectively disclose to other providers and researchers.

Consider a Patient visiting a Primary Care Physician and an ER Doctor. The Primary Care Physician and ER Doctor use different EHR software providers (e.g. AthenaHealth and NueMD) in which they have invested time, money, and information. After the Primary Care Physician and ER Doctor install a plugin to AthenaHealth and NueMD, they do not have to change their behavior or process for recording patient information. The care providers and EHR providers are able to maintain their existing infrastructure and investments. With the permission of the patient, providers are also able to access time-stamped, verified information the patient has stored including over-the-counter and prescription drug usage, data from personal devices (blood glucose level, heart rate, etc.), and more.

Whenever the Primary Care Physician opens, views, or edits the medical record for the Patient on their AthenaHealth software, the software encrypts the information from the interaction using the Patient's public key (when the Primary Care Physician encrypts data using the Patient's public key, only the Patient can decrypt the data using his/her private key). IPFS stores the encrypted information and produces a hash of the data (a hash is the unique data fingerprint). A hash can be stored publicly in a smart contract because data cannot be interpreted from its hash.

A patient-specific smart contract stores timestamped hashes from the patient and all of his/her care providers, thereby providing a secure, longitudinal medical history created by all of the stakeholders in a patient's health. A medical provider automatically has access only to the information s/he created on the patient's record (before it is encrypted), and the patient automatically has access to all of the information stored in the smart contract (because all information is encrypted with the patient's public key, and therefore can only be decrypted with his/her private key).



Because the patient has access to all of the hashes' underlying data, s/he can decrypt and then re-encrypt the information with an ER Doctor's public key to share their current and complete medical history with the ER Doctor. This way the ER Doctor has an up-to-date medical history of the patient at the time of their procedure, but will not be able to read further updates unless the patient again chooses to disclose them.

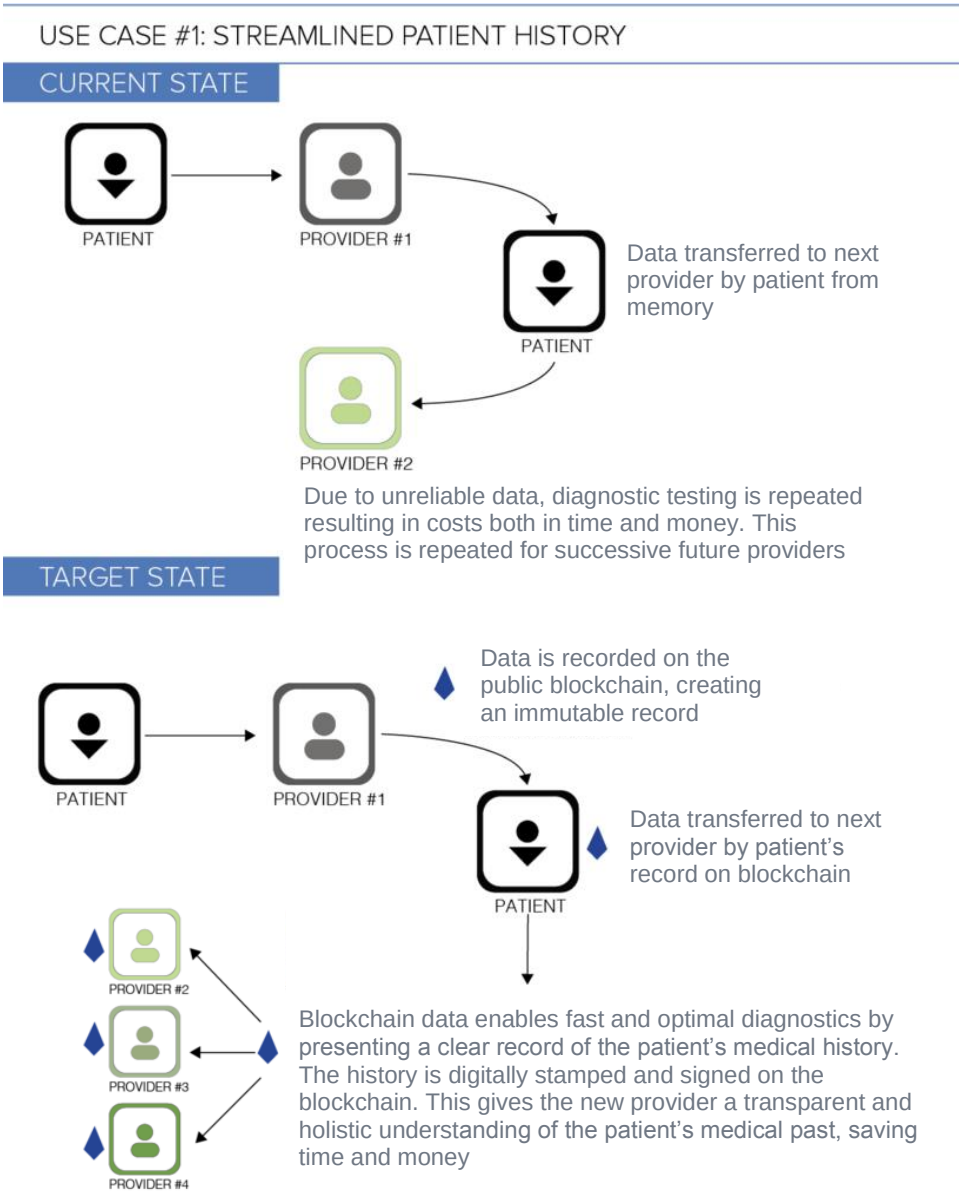
This architecture provides patients with an immutable, longitudinal health record that grows with them. Patients have access to all of their information at all times, and have the ability to share a copy of their complete record or selectively disclose certain aspects of their record to authorized parties. When a patient shares a copy of their record, they are not sharing the record itself, but taking the information that exists in the record at that instance, decrypting it with their public key, and then re-encrypting it with the public key of the intended receiver to send across the network. This way, care providers only maintain records of patients up to their most recent appointment with the patient, just like they have to-date. However, when a patient visits a care provider for his/her next appointment, s/he can instantly update his/her care provider on other health events that took place since his/her previous visit.

Because the proposed architecture is a backend solution that uses the interface of existing EHR platforms, it will require little to no change in user behavior. After the initial installation of the plugin, care providers will continue to evaluate medical events as they always have while the recordation of data on the blockchain takes place automatically. Patients will have the opportunity to add progress updates, symptoms, and reviews of their medical experience on their own record. Updates that occur between patient visits will be time-stamped, directing the provider's attention to new information that has been added to the record. With many stakeholders equally participating in the development of a longitudinal health record that centralizes patient care, educated consumers will begin to make decisions that value quality over quantity of care. This may force the market to shift from fee-for-service to value-based payment policies.

Regarding the security of a system which pushes patient data from private databases at network edges to encrypted public storage intrinsic to the network itself: such a design will be more secure by far than any existing centralized security infrastructure. Even the best centralized security infrastructure is subject to insider attacks which can leak the information of every patient administered by the hospital, practice or provider in question. Fundamentally, central points of security failure are made to disappear by transferring data encryption keys from providers to patients. The most disastrous security breach cannot leak more than one patient's data in this model, and such a target is less attractive than the honeypot databases maintained by large hospitals and provider networks. The AES algorithm with which data may be encrypted in such a system is mathematically sound, resilient to quantum cryptanalysis and approved for use in transmitting and storing top-secret data by the US Government.

4.1 USER STORIES

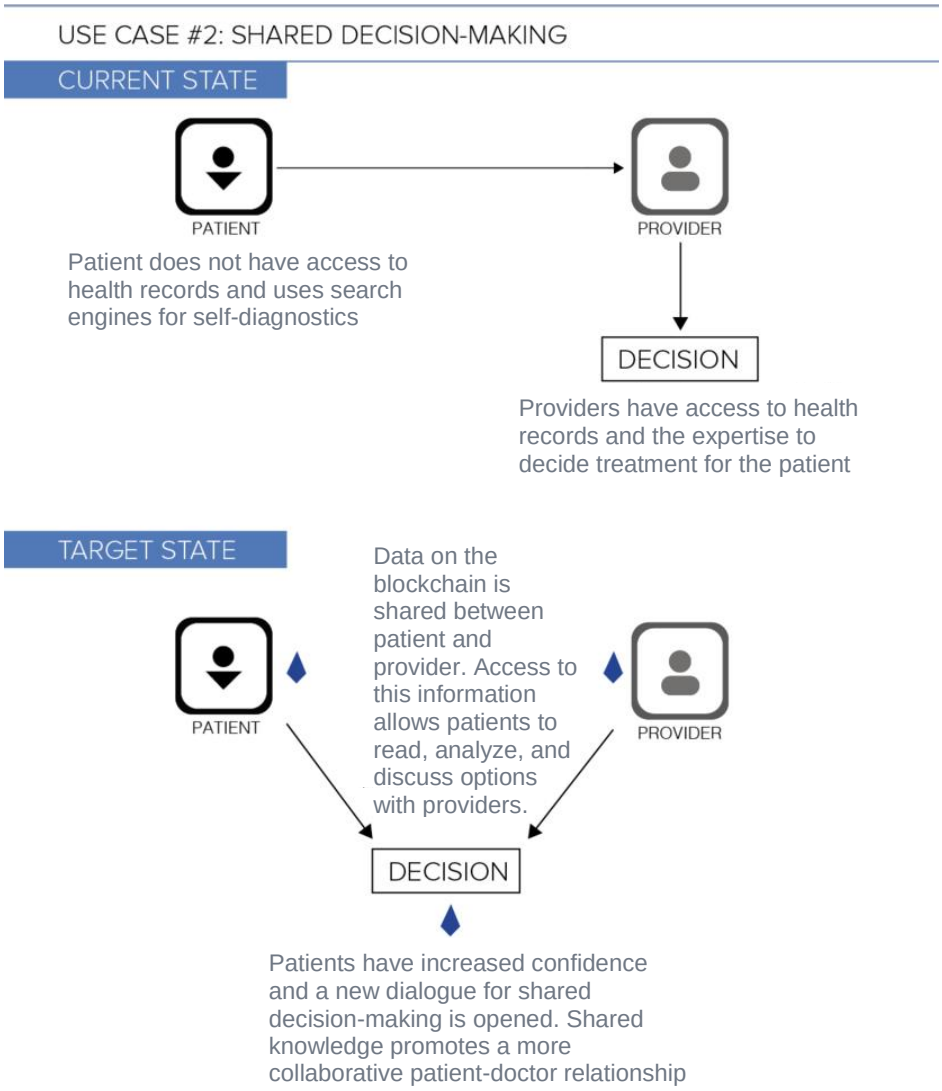
User Story 1: *Streamlining the information recordation process to improve accuracy, reduce costs, and eliminate time-waste*



Current State: Presently, when a patient first visits a care provider or changes care providers, they have to transcribe pages of personal identity and medical information from memory. This process provides no assurances about the integrity or completeness of the data transcribed. While some data sharing occurs between practitioners with the permission of the patient, it is inefficient. In practice, for a patient to share their medical history with the provider caring for them they mostly have to rely on their memory and their personal understanding of their health, which varies in accuracy from patient to patient. As a result, there develops a disconnect between the actual state of a

patient, and the state of a patient that a physician perceives. With the importance of understanding a patient's current and historical medical standing, care providers need a more reliable method for learning about the history of a patient. Moreover, without legitimate documentation substantiating a patient's claims, providers are required to repeat diagnostic tests, which wastes time and money. Medical claims processing is also labor-intensive and can be further slowed down by lack of proper documentation or fraudulent claims.

Target State: When a patient arrives at a care provider's office, they instantly share a copy of their aggregated EHR with the doctor, which the doctor can access through his/her existing EHR infrastructure. The record includes: insurance information, pharmaceutical information, data recorded on the patient's smartphone medical applications, logs the patient has made, medical information that the patient's other care providers recorded about the patient, etc. all timestamped and digitally signed. This record not only solves the problem of medication list management, but also provides the care provider with a longitudinal picture of the patient's health, not just unsubstantiated claims and episodes of care. With a streamlined, verified, and auditable patient history, claims processing is made more efficient. Due to complete and verified documentation, claims can be processed immediately with no intervening correspondence or wait times. The number of appeals are also drastically reduced.



User Story 2: *Informed Choice and Completeness of Records*

Current State: Patients often are asked to make health decisions without the opportunity to holistically reflect on their full medical standing. As a result, patients turn to incomplete information or the generic results of search engines in an attempt to compensate for their dearth of knowledge. They make personal, life-altering

decisions based on limited facts or impersonal articles that they first read with decisions impending. As a consequence, patients may make uninformed judgements based on search engine results without a complete patient data-centered decision making process. In a Canadian study of patient preferences for knee replacement surgery (Hawker et al. 2001), only 15 percent of the patients clinically eligible for surgery preferred to enter the Operating Room. If the remaining 85 percent of candidates felt educated and informed enough to initiate a conversation with their doctor to confidently reject the surgery, huge treatment and time costs for the doctors and patients would have been conserved. Because patients do not have a longitudinal view of their personal health, they are unable to make confident, educated decisions about their survival.

Additionally, with the technological advancements of the BYOD and mHealth era, healthcare has been afforded new possibilities. However, hospitals are finding it challenging to update their security policies to keep up with these advancements and physicians are cautious of data overload. Therefore, data from mobile medical applications and wearables go largely unused by physicians when making decisions about the health of a patient. While the application of IoT in healthcare and the accuracy of personal wearables are still under scrutiny, it is undeniable that real-time data and constant monitoring can lead to new insights about a patient's health. The usage of wearables in the detection of abnormal heart beat and early stroke have been detailed in the *Annals of Emergency Medicine*. Unfortunately, given the previously mentioned barriers, IoT in healthcare still faces limited adoption.

Target State: A health record that patients can read, evaluate, and discuss constantly with their care providers lays the foundation for long-term knowledge. They can confidently and knowledgeably approach their care providers with questions throughout their relationship. In consequence, when there is no clear option for best treatment, patients have an improved information base to use to form a more collaborative patient-doctor relationship from which to work, empowering them to be educated decision makers.

As part of this improved information base, data from a patient's mobile medical applications and wearables are automatically added to his/her record on the blockchain. With the permission of the patient, physicians can easily access this data with his/her public key in the same way s/he would view more traditional medical records on the blockchain. The IoT data is secured through the same rigorous encryption method applied to any other record, as previously detailed. Therefore, hospitals do not need to create new security policies surrounding IoT data alone, physicians can easily access IoT data without leaving their preferred systems, and researchers are able to apply machine learning to the influx of new data, allowing for more advanced approaches towards predictive diagnoses. Increased usage of IoT data will also push IoT producers to improve their products, leading to greater accuracy and usability of IoT data.

User Story 3: *Patient Centered Outcomes Research and Precision Medicine*

Current State: PCORI-funded clinical trials provide participants with informed consent documents, which participants sign prior to participating in a clinical study. Informed consent information and participant signatures, however, do not grow with the patient throughout their clinical process. Although patients can remove themselves from trials at any time, they lack assurance that they are comfortable and educated as the trial progresses.

An institutional review board (IRB) reviews, approves, and monitors every federally supported or conducted clinical study and drug, biological product, or medical device study regulated by the FDA. The IRB ensures the minimization of research risks and reviews the informed consent document. Multiple regulators including data monitoring committees, the Office of Human Subjects Research, and the FDA authorize the

protection of participants throughout the clinical studies. While enrolled in a clinical study, participants typically continue to see their usual healthcare providers. The participant in the clinical trial is solely responsible for educating their usual healthcare providers with information on the clinical study and ensuring that the study protocol will not conflict with other medications or treatments.

There are many parties attempting to ensure the safety of a patient undergoing clinical trials. However, the patient is the sole information provider to these many entities, and patients do not have a secure, well-rounded understanding of their health because they can neither access nor share their records seamlessly. Because patient centered outcomes research leads to precision medicine, the research needs a method to obtain more reliable and secure medical information.

Target State: With the simple click of a button, a patient selectively discloses medical information on their personal health record. Patients have the ability to share relevant medical data with researchers without revealing their identity. Researchers seamlessly use the data to analyze a patient's health and personal history, and make lifestyle, medication, and clinical trial recommendations to patients and their healthcare providers by communicating them on a patient's personal health record. A patient has all of their health information and interactions in one place, easing the process of education, communication, and regulation for all involved parties.

5 FUNCTIONALITY IN THE "REAL WORLD"

The technology to support the proposed solution is already in existence. The efficiency, security, and auditability of the Ethereum blockchain have been verified in the financial sector through different large-scale tests run by financial institutions including Wells Fargo, UBS, and TD Bank, to name a few. These examples have successfully demonstrated the effectiveness of blockchain solutions and the ability of these solutions to function in the real world. While the technology is ready to be applied to healthcare, the main implementation issue that our proposed solution must face is buy-in from patients and providers.

Without the support of patients and providers, the benefits of the proposed blockchain solution cannot be fully realized. Gaining acceptance for the solution will require the education of individuals to ensure that they not only understand how to record and access information on the blockchain but also understand how to truly leverage the new capabilities offered. Individuals do not need to understand the complexities of the underlying technology to be able to benefit from it; the internet is fully understood by very few people but enhances the lives of the large majority of the United States population. Individuals will, however, need to understand how to interface with blockchain through mobile apps and EHR systems as previously proposed, similar to how people needed to learn to use web browsers such as Internet Explorer.

Assuming there is buy-in from key stakeholders, implementation may still prove to be a labor-intensive process given the need for the creation of patches to transfer patient records from existing EHR systems to the blockchain. Once a patient's history has been verified and recorded on the blockchain, the sharing and updating of that history can flow smoothly. However, getting to the initial state of having a base record on the blockchain will require time and effort. The transfer of data must be secure to protect PHI and PII. Whether it is the patient's responsibility to transfer the data, the provider's responsibility, or the EHR provider's responsibility will also have to be determined.

Initial investment cost implications will include the build cost for the solution's infrastructure, the cost of transferring existing medical data to the blockchain, and the cost of training providers and patients to use the new solution. The build and transfer costs will contribute to the majority of the total cost. Some education and preparation is needed but should be limited, as physicians will be interacting with the same

EHR interfaces they are already familiar with. Because the solution piggybacks on existing EHR infrastructure, hardware costs are eliminated. Operations and sustainment costs will include licensing, hosting, and technical support costs. As with existing solutions, these O&S costs will be vendor-dependent. Compared to EHR maintenance costs, maintenance costs for the proposed blockchain solution should be lower due to the inherent automation and fault-proofness of blockchains. The proposed blockchain solution promises to provide greater interoperability, efficiency, security, and less fraud, causing the benefits to outweigh the costs.

6 CONCLUSION

Booz Allen, ConsenSys, and Microsoft propose a solution in which patients, medical devices, smartphone applications, researchers, healthcare providers, and other healthcare stakeholders are identities on the blockchain contributing to and learning from a longitudinal healthcare record with cryptographic security, without a single point of failure. Our solution maintains the existing Health IT infrastructure by offering blockchain as a plugin and backend service to electronic health record providers. By utilizing existing systems, previous time and financial investments made by healthcare stakeholders continue to be worthwhile and little to no user interface or behavioral changes are required. Without changing behavior, blockchain can streamline the information recordation process to improve accuracy, reduce costs, and eliminate time-waste while establishing a framework for informed choice, shared decision-making, patient-centered outcomes research, and precision medicine.

Patients will become the center of their care because they are the gatekeepers of their medical data. Although multiple entities can easily contribute to a patient's health record, they do so without the ability to access the patient's complete record. Only a patient can grant selective or complete access to a copy of their personal record. By granting access to a copy of the record and not the record itself, the patient is empowered to switch providers as s/he sees fit. A patient seeking care has the power of any consumer seeking a service in a competitive market, which financially incentivizes a shift toward value-based payment policies.

7 RESOURCES:

1https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

2 http://www.ncbi.nlm.nih.gov/books/NBK53487/

3 http://www.pcori.org/research-results/patient-centered-outcomes-research

4 https://clinicaltrials.gov/ct2/about-studies/learn