Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

May 2017

This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in Patientory or any related or associated company. Any such offer or solicitation will be made only by means of a confidential offering memorandum and in accordance with the terms of all applicable securities and other laws.

Abstract

A blockchain powered health information exchange (HIE) can unlock the true value of interoperability and cyber security. This system has the potential to eliminate the friction and costs of current third party intermediaries, when considering population health management. There are promises of improved data integrity, reduced transaction costs, decentralization and disintermediation of trust. Being able to coordinate patient care via a blockchain HIE essentially alleviates unnecessary services and duplicate tests with lowering costs and improvements in efficiencies of the continuum care cycle, while adhering to all HIPAA rules and standards. A patient-centered protocol supported by blockchain technology, Patientory is changing the way healthcare stakeholders manage electronic medical data and interact with clinical care teams.

1 Introduction

1.1 What is Blockchain?

The technology behind the bitcoin digital currency, blockchain's birth is traced to the pseudonymous, unidentified person (or group) known as Satoshi Nakamoto. Since 2009 blockchain has gained more widespread use in the finance industry, with a variety of new blockchain-enabled businesses and services entering the market. Blockchain's technology is used to share a ledger of transactions across a business network without control by any single entity. The distributed ledger makes it easier to create cost-efficient commercial relationships where virtually anything of value that can be tracked and traded without requiring a central point of control. The technology puts privacy and control of data in the hands of the individual. Trust and integrity is established without reliance on third-party intermediaries.

1.2 Current Healthcare Infrastructure

The realignment from a "procedure" based focus to "holistic care of the individual" requires Care Providers form "networks" that work together towards a common goal of improving the care outcome of patients under care, for post-acute care episodes or between acute care episodes. The need for cooperation between care-providers ranging from specialists, primary care physicians, caregivers and wellness providers (like nutritionist and rehabilitation nurses) results in increasing use of digital technologies. Though these solutions have significantly improved the tracking and efficiency for delivering care, they have resulted in creating silos of health information, primarily within electronic medical records (EMR) systems.

Health and government organizations spend a significant amount of time and money setting up and managing traditional information systems and data exchanges; requiring resources to continuously troubleshoot issues, update field parameters, perform backup and recovery measures, and extract information for reporting purposes.

Federal laws and incentive programs have made health care data more accessible, in response to hospital pushback regarding EMR implementation. However, the vast majority of hospital systems still can't easily (or safely) share their data. As a result, doctors are spending more time typing than actually talking to patients. Physician burnouts jumped from 45 to 54 percent between 2011 and 2014 [1].

Although there exists the notion of "individualized" health information both on the clinical as well as wellness front, these have not translated into "personalized" plans of care. Furthermore, even though there is a plethora of data, the overall healthcare ecosystem is incapable of adequately engineering a value or risk to big data to help better predict future care episodes of a patient.

Hence the current solutions pursued by the Health Care technology industry have resulted in a difficult choice between care and privacy/economic fraud for patients. We see this issue greatly expanding as more data is being created by the industry. **Blockchain's secure technology, properties, and distributed nature can help reduce the cost and efficiency of these operations as well as provide a viable security infrastructure.**

1.3 Patient-Provider Relationship

The new healthcare paradigm demands the need for effective and optimal care delivery for patients to yield better care outcomes. This requires that Principal Care providers are able to actively coordinate and collaborate with other care providers involved and ancillary health organizations like Labs and Pharmacies in care delivery. Ultimately, for this to be successfully patient records need to be updated and modified in a timely manner.

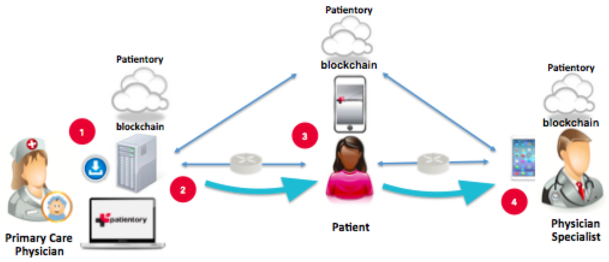

Figure 1: Patientory Schematic

EMR software currently prohibits an effective patient-provider relationship. Patient portals have minimal engagement among patients, as a result of the siloed patient experience. Furthermore, this software only provides a limited capability of exchange of information from one system to another and usually requires a designated individual who is capable of such information transfer. This has led to an increasing amount of delay between organizations in delivering care for the patient and also resulted in the overall decrease in quality of delivery of care services to the patient. Also, as care providers are spending more of their time involved in coordination of care, their effectiveness in treatment of patients and workload has significantly increased. This has resulted in a counter-intuitive impact in care outcomes for patients.

In addition, given that many doctors don't want patients to access EHRs, patients adopt a passive role in tracking their health. This ultimately makes them feel a lack of control and ownership of their health leading to the patient becoming frustrated and being disengaged in their care. Though there is a recent increase in Mobile Health Care apps helping individuals track their vitals and health parameters, the novelty has not translated to improved patient care or adherence and outcomes as it too faces the challenges of getting integrated into EHRs.

2 System Overview

These current issues are solved using the Patientory Blockchain Network. Legacy EMR are centralized structures subject to hacking, strict security regulations, and onerous overhead costs. By implementing the Patientory Blockchain infrastructure, providers will see minimized breaches due to the inherent access control properties of the system; a channel for facilitated care coordination with results in overall improvement in health outcomes. Above is a schematic describing the Patientory blockchain infrastructure and its interoperability among patients and their providers.

3 System Implementation

3.1 HIPAA Regulations and Compliance Guidelines

Prior to any meaningful discussion of implementations, the restrictions enforced by the mandates of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must be addressed. Those rules of primary concern are the Privacy Rule, the Security Rule, and the Cloud Computing Guidelines. The intent of this paper is not to perform a full investigation of HIPAA law. Those elements that are pertinent to the implementation discussion shall be defined and further discussed upon the moment of relevant application.

A. Privacy Rule

The business model of Patientory provides that the Privacy Rule requirements must be observed due to the electronic storage and transmission of private health information. Applicability of the privacy rule is summarized as, "The Privacy Rule... (applies) to health plans, health care clearinghouses, and to any healthcare provider who transmits health information in electronic form" [2]. In addition to these agents, those parties that act on their behalf, as service providers, are also responsible for HIPAA compliance. These second hand agents are termed Business Associates (BA), and the legal document that defines the rules and regulations that the BA must adhere to is termed Business Associate Contract (BAC). HIPAA places strict requirements on the nature of these agreements.

The points of merit, from an initial investigation, are those requirements that specify the authorization of use, the use of de-identified information, and the definition of private information. Private health information (PHI or ePHI for electronic data) is defined as "all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral"[2]. De-Identified health information is defined as "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information" [2]. De-Identified data use restrictions are summarized by the following, "There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual" [3]. The boundary of identifiable data to de-identifiable data is defined as any information that may restrict the possible number of individuals a collection of information is associated with to less than 0.04% of the total US population.

B. Security Rule and Cloud Computing Guidelines

Due to the length of the content associated with this topic, only those elements of primary concern are isolated for reference. These primary concerns are as follows, "When a covered entity engages the services of a CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate under HIPAA. Further, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data. Lacking an encryption key does not exempt a CSP from business associate status and obligations under the HIPAA Rules. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules" [3].

Covered entities often use cloud storage providers (CSPs) to store health information, often citing that it is more cost effective and there are lower IT management costs. However, as consumers rely on cloud providers to store personal data, they relinquish direct control over that data and, as a result are unaware of who has access and where the data is geographically located. Even if an explicit business associate agreement is developed between the BA and the cloud storage provider, it would only provide the terms of who takes responsibility of the privacy and security of the data in the event a breach occurs. The consumer would potentially have control over access to these data streams, but would rely on the cloud storage provider to enforce those privileges.

Although the use of cloud storage is popular, there are still a number of risks that a consumer undertakes when using this mechanism for their personal data. In cloud-based architecture, data is replicated and moved frequently, so the risks of unauthorized data use increases. Additionally, multiple individuals are granted potential access to the data, such as administrators, network engineers, and technical experts that perform services on, or for, the servers that host this data. This also increases the risk of unauthorized access and use.

However, even if the data is secure through strict access controls and is encrypted at its point of origin and while in transit, it still poses a problem for the development of Patient-Reported Outcomes Measures (PROMs). The concept of a PROM is to develop a patient-focused measure that relates to an area or focus that is of concern to the patient, and one in which their engagement and feedback is essential for its successful implementation. Accessing large data streams from a variety of devices that are part of the IoT network, as used now, in conjunction with cloud based services can provide a foundation on which to base a PROM, but it is difficult to know whether that data siloed in the cloud will produce a measure that will have the intended meaning and relevancy for a patient.

Implementation of blockchain technology to ensure and enhance data security for all the medical records associated with the system can minimize health breaches and ultimate decentralization of record ownership. The process of encrypting data when sent to database using different algorithms and decrypting it during the retrieval will be used.Data shall be encrypted using NIST compliant algorithms during transmission and retrieval as is mandated by law. Thus, all exchange of information will comply with those best practices outlined in the NIST specifications.

In regards to the rapid growing number of data breaches facing the healthcare industry, blockchain technology makes HIPAA compliance

feasible for both patients and providers.

C. Blockchain System Analysis of Limitations due to HIPAA Restrictions

The Ethereum Blockchain facilitates a diverse subset of system implementations due to the application of a Turing complete programming language that is executed on the Ethereum Virtual Machine. These systems have limitations in that the virtual machine has no direct outward facing inspection of the broader internet except through the use of Oracle Services. Additionally, the storage limitations of the blockchain are enforced by the gas cost of storage and gas cost of access to this data. As of this writing, the block time of the chain establishes a minimum bound for state modifying requests of at least fifteen seconds.

The limitation of the blockchain to host private information may be overcome through data obfuscation, such as encryption, but in the event that the decryption key is ever leaked, there is no way to remove the sensitive data itself from the blockchain. For the purpose of HIPAA compliant data, this may potentially result in a persistent, uncorrectable leak of information due to the immutability of the blockchain itself. Although de-identified data may, in theory, be stored on the Public Ethereum Blockchain, it would be disastrous to assume that the de-identification filtering mechanism will never fail, or that the sideband information associated with blockchain interactions can not inadvertently reveal identity. This conclusion was also reached by the MIT Media Lab during the formation of the MedRec Protocols and summarized in the MedRec Whitepaper [3]. Mining this sideband information may be as simple as observing timestamps and interactions with known data storage contracts.

Through this analysis it may be possible to associate an individual with an institution, and more importantly the time during which they were present at a facility. Given the specialized nature of some facilities, this is enough information to constitute a violation of HIPAA compliance due to a passive observer's ability to infer both identity, location, time of interaction, and possibly, class of diagnosis.

Pending that this location is remote in nature, the reduction to less than 0.04% of the US population becomes trivial. These facts constitute unreasonable single point failures that must be acknowledged. Further, the direct storage of even encrypted information on the blockchain creates a responsibility of the database managers to enter into a BAC due to their actions as a HIPAA data storage facility (See section titled Security Rule and Cloud Computing Guidelines). This is an unreasonable expectation since every miner, and even those individuals hosting passive nodes, would all need be HIPAA compliant. Due to these concerns, we implement a mechanism for the persistent storage of sensitive information through the use a private implementation of an Ethereum based blockchain.

D. Implementation Goals for Usability and Security

The primary goals of any secure system may be summarized as the goals of confidentiality, integrity, availability, accountability and information/identity assurance. In order to accommodate these goals an attacker and user must be defined. Each of these roles demands certain acknowledgements of ability. From the perspective of the user, the system need be sufficiently transparent that no advanced knowledge is needed. Also, due to the inability of the normal user to grasp the complex considerations of cybersecurity, the process needs to be resistant to the actions of the user.

In the event that an attack does occur, the system is created such that the amount of effort that must be invested to compromise a resource is worth more than the value of the resource itself. This is due to the realization that a sufficiently advanced party with appropriate resources will always be capable of violating any system, given enough time and effort. More compactly, there is no perfect defense. With these restrictions in mind, the implementation itself may now be discussed such that we achieve all of the goals previously mentioned.

3.2 Definition of Hardware and Network Implementation

To accommodate the above stated design goals, the selected system implementation requires several independent systems. Each system subdivides authority, ensures only authorized entities may interact in an approved manner, and provides a mechanism to increase security while maintaining availability. This system has also been devised such that scaling may be readily accomplished through the addition of hierarchical calling schemes. These systems are fully described in detail below.

The public facing entity is a Remote Procedure Call (RPC) Server that acts as an interface to a private implementation of the Ethereum Blockchain (permissioned blockchain). This network of blockchain nodes, is only authorized to interact with the other blockchain nodes, a key authoring entity, the HIPAA compliant storage facility, and the RPC Server. The key authoring entity is the resource that generates private/public key pairs for use on the blockchain. The HIPAA compliant storage facility hosts the actual data that constitutes electronic private health information (ePHI).

When a request for data does occur, the HIPAA compliant system may be authorized to speak to the forwarding agent, who then re-routes data back to the RPC server. Alternatively, it may be structured such that the HIPAA storage speaks directly to the RPC server. Each implementation has benefits that must be considered prior to final selection. In either event, the HIPAA storage facility decrypts the relevant portions of the database upon request handling. This decrypted information is then re-encrypted using the public key of the requesting party for transmission. This public key is also the public key of the contract that acts as the control interface from the blockchain to the HIPAA data.

The diagram of the specified network topology may be seen at figure 2.

3.3 Definition of Software Implementation

In addition to the physical isolation of systems in the hardware and network implementation, software access control facilitates the integrity of data and

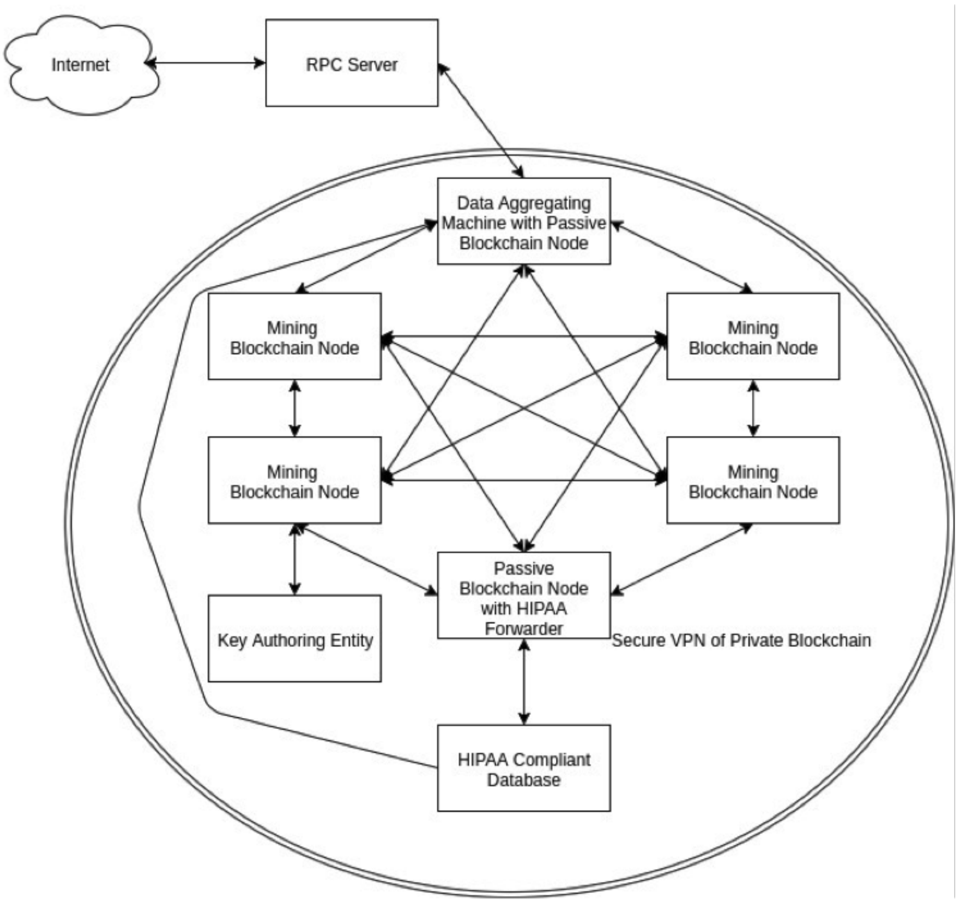

Figure 2: Patientory Blockchain Network Topography

verification of authorization for requesting entities. The software system, from the perspective of access control and data encryption is described below.

The HIPAA compliant database will only accept inbound connections from the HIPAA forwarder. This ensures that the flow of traffic is isolated to known controlled paths. The HIPAA forwarder will only act to forward a request to the HIPAA storage facility pending a valid transaction has occurred on the blockchain, and this transaction resulted in the emission of a requesting event. This requesting event need contain the public key of the requesting party, and those data fields being requested. Finally, the RPC server uses an access controlled Application program interface (API) such that only known users may interact with the server.

In order to understand the call hierarchy of the system, the contract structure to facilitate access control must first be addressed. Every user in the system maps to a private address on the private blockchain. Every private address is only authorized to directly speak to ONE contract on the block chain. This contract is the individual's class contract. Institutions, institution employees, and customers are class level objects.

These class level objects are permission-based interfaces. The Institution Contract has a list of all customers that have granted viewing privileges to the institution and each customer contract has a list of all institutions that it has granted permission to. The contract held by the institution has functions that facilitate any revocation of permissions to the institution, from the user. **The institution contract may not self alter this list, thus preventing unauthorized access to individuals' records.** Additionally, the Institution Contract possesses a list of authorized employees that it is fully capable of maintaining. This permission scheme should ideally function such that automatic revocation of a permission is performed at semi-regular intervals to prevent an institution from inadvertently preserving former employees' access rights.

Within this system, all external parties interact through the submission of signed transactions that encode the requesting call. These transactions are submitted through the RPC server upon user validation. The RPC server posts these requests to the data aggregation server who then forwards these requests to the miners based on a load sharing mechanism. The miners then process the request by submitting the transaction on behalf of the calling party to the party's respective controlling contract. This contract holds the permissions of the data that the entity is authorized to access internal to the contract. This contract is the only entity that will accept a transaction from an outside request. Thus, a mechanism is established to fully control call operations on the blockchain.

For any given transaction, an immutable record of the calling party is created. This ensures that all attempts to access information are recorded. The actual data stored within the user contract is a system of hash pointers that when resolved by the HIPAA storage server result in the return of the appropriate data. This information is bubbled up to the HIPAA forwarder by the execution of a valid request transaction. The mechanism that facilitates this communication is indirect and manifests through the blockchain event messaging system. Due to the limitation that the requester may only query the database by valid transaction, and the user may not directly alter their own information, access control is provable. From the perspective of institutions, the mechanisms are similar except the institution contract hosts a list of users from whom it may request data and a list of users who may interact with this institution as employees. When a request transaction originates from the contract of an institution employee, the controlling contract calls the institution contract, who calls the user contract to ask for the data pointers that resolve ePHI. Pending the institution is on the list of approved institutions for the user, the contract returns the appropriate hash pointers. These pointers are then published as an event message that again bubbles up to the HIPAA storage facility.

For clarity, the full process of a single request is as follows: The external party requests data from the service by calling the RPC server with a cryptographically signed transaction for submission to the blockchain. The RPC server verifies the external party's identity via the signature of a login request.

Pending the signature matches an entry in the database of permissioned public keys, the RPC server accepts the request and submits the request to the Data Aggregate Machine. The Data Aggregate Machine then submits the requests to the private blockchain verifiers. The verifiers receive the request as a call from a blockchain account against a target contract. The verifiers execute this call, and in the event that the request is an allowable action, the transaction is entered in the next block. This transaction also causes the emission of an event message in the blockchain. This event message is observed by the HIPAA Forwarder, who acts to create an encrypted request against the HIPAA storage based on the hashes of the event message. This message also contains the public key of the requesting party. The HIPAA compliant database system observes this request and transmits an encrypted copy of the information to the RPC server using the public key of the requesting party. The RPC server then returns this information to the requesting party by remapping the requesting IP to the public key in the message. The RPC server transmits this message without ever having seen the underlying data. This data is then immediately destroyed by the RPC server, thus ensuring that the RPC server acts as a conduit that need not be HIPAA compliant.

The mechanism to publish data is again similar in nature, but the data that is to be submitted is encrypted with the public key of the HIPAA storage facility. The other operations are identical except the data that is being posted bubbles up through the event message system. Thus, due to the use of low collision hashing functions and timestamped nonces, data may be stored with the contract being capable of computing the address at which submitted data is located within the HIPAA storage facility.

Finally, the distribution of private keys to entities must be addressed. This may be facilitated through optical means to smartphone users. This is analogous to the use of QR codes as addresses for Ethereum addresses. Alternate means may also be established using applications on both desktop computers and tablet/smartphone devices. The loss of a key is not a catastrophic event, due to the ability to administratively strip a controlling contract's access control from one key and grant it to another.

3.4 Interoperability

EHR systems are based on an isolated credential validation architecture in which patient data is kept in each of the separate systems. This has resulted in one-to-one care co-ordination software "add-ons" solutions to these systems to enable the coordination of care across other providers and ancillary health organizations. However, the access of the information from the principal Provider organization to the other organizations is only via limited capability in instances such as to Read, to Submit, to Send or to Notify. Furthermore, the Patient/Consumer has very limited interaction or involvement in this exchange of information. In addition, a drawback to the existent mechanisms of data exchange is the difficulty in rectification of errors that occur during the submission process.

Once a blockchain and its smart contracts are configured, the parameters become absolute. The patient becomes the primary intermediary in sending and receiving health information negating the need for frequent updates and troubleshooting of any software. Since blockchain records are also immutable and stored across all participating users, recovery contingencies are unnecessary. Moreover, blockchain's transparent information structure could abolish many data exchange integration points and time consuming reporting activities.

3.5 Processes and Scalability

Users are in control of all their information and transfers which ensures high quality data which is complete, consistent, timely, accurate, and widely available thus making it durable and reliable. Due to the decentralized database, blockchain does not have a central point of failure and is better able to withstand malicious attacks.

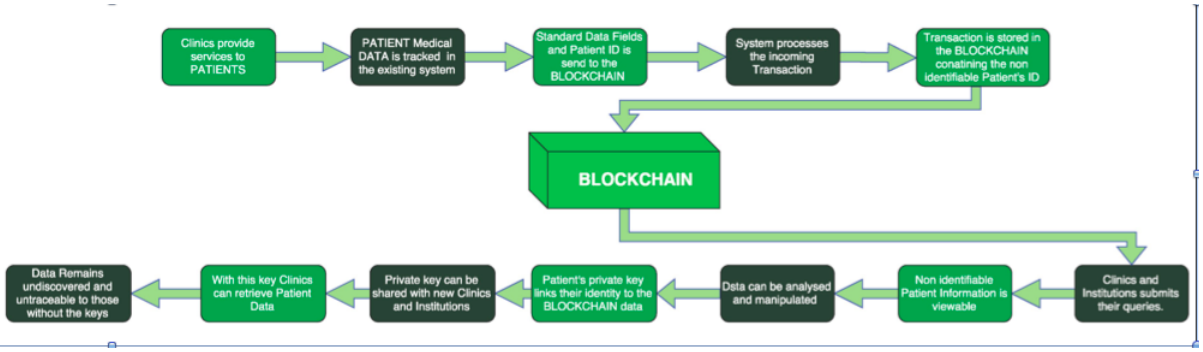
Clinics provide services to PATIENTS
PATIENT Medical DATA is tracked in the existing system
Standard Data Fields and Patient ID is send to the BLOCKCHAIN
System processes the incoming Transaction
Transaction is stored in the BLOCKCHAIN conatining the non identifiable Patient's ID
BLOCKCHAIN
Clinics and Institutions submits their queries.
Non identifiable Patient Information is viewable
Dsta can be analysed and manipulated
Patient's private key links their identity to the BLOCKCHAIN data
Private key can be shared with new Clinics and Institutions
With this key Clinics can retrieve Patient Data
Data Remains undiscovered and untraceable to those without the keys

Figure 3: Blockchain Process Flow Diagram

In any Care network it is necessary to ensure that participants who are collaborating together can depend on each other to deliver the necessary services that are expected of them. To achieve that, there has to be a means to ensure accountability of task and services that are expected to be delivered in a timely manner and also associated liability if they are not delivered in a timely manner at the level of quality that is expected. Hence, any Health Care infrastructure has to be capable of seamlessly being able to monitor the necessary information to enable the Primary Care Provider to evaluate his Care network. Furthermore, as the Care network grows and these interaction between network care providers increase the Health Care infrastructure should be capable of effectively addressing this scale.

The key aspect to building a highly scalable and distributed Care Management system is a peer-to-peer architectural framework. Such a framework has already been used in a number of industry segments like, media, sports, real estate, supply-chain, displaying blockchain can easily be an add-on software connector to existing centralized frameworks[7]. This has led us to explore using the block chain framework for its applicability to help with enabling a peer-to-peer framework for healthcare.

Block-chain holds the promise of validating two or more entities engaged in a "healthcare transaction". This provides two key attributes compared to a centralized authentication model. The first being, that interested parties can engage with each other at a "transaction level" of "trust relationship". The second is that the liability exposure in such a relationship is limited to only "transaction level" engagement. This is very useful as it limits the access of information and liabilities between parties involved and at the same time enables a party to get into a transaction relationship with a number of other providers based on their specific capabilities and type of care to be delivered to the patient. This is significantly better than a conventional centralized systems needing to limit the number of providers for a wide range of patient needs due to effort required to manage the access and liabilities.

3.6 Health Information Exchange and Tokens

The Patientory token (PTOY) is the fuel for driving the blockchain infrastructure. The primary usage of the token is to regulate network storage allocation, health care quality measures and revenue payment cycles.

Patients are given an allotted amount of space to store information for free on the Patientory network. PTOY allows them to purchase extra storage space from nodes set up in hospitals systems. PTOY can be purchased via the platform or an exchange.

Healthcare organizations use PTOY in this instance as well. It is also used in payments once smart contracts are executed with healthcare insurance companies and serves as a mechanism to regulate value based model metrics.

In order for the US to successfully move away from the fee-for-service model to the current value-based model, there has to be a healthcare IT infrastructure that allows organizations to link quality, value and effectiveness of medical interventions through a reputable compensation model.

Compensation will be based on how effective the network of providers' work together to ensure improvement in the quality of care and wellness outcomes, while at the same time reducing associated care cost. To truly incentivize different participants in the network to pro-actively create better care regimes, a merit based compensation of shared savings (reimbursements) takes effect. In order to effectively allocate a proportionate share to the provider in the network that contributed the most towards the overall savings, a clear tracking of their contribution is measurable executed by smart contracts on the blockchain network .

Another key impact of the new healthcare paradigm is the compensation model where-in the providers are eligible for receiving additional compensation beyond the care delivered. This compensation is the result of savings that are generated based on how effectively the providers manage the care of the patient's health outcome (incentives). Any savings generated through efficient management of the patient's care can be retained by the providers and their network partners as part of the shared savings aspect of the new healthcare paradigm.

Our proposal renders the ability for payors to transfer tokens as incentives to providers that achieve these quality metrics. The ability to seamlessly track and manage smart contracts in which the benefits can be redeemed with significant ease provides the necessary "carrot" for providers and patients to actively engage in a symbiotic collaboration. Contrarily, if one or more participants falters appropriate penalties, via liabilities, can also be levied with similar ease. This "carrot/stick" approach will provide the necessary push that is needed to shift the healthcare industry from a sickness management mindset to a wellness lifestyle mindset.

Henceforth, Patientory issued tokens (PTOY), is the native token of the Patientory platform. In exchange of PTOY tokens, users will be able to use the network to rent health information storage space, and to execute health specific smart contract payments and transactions.

We firmly believe that using a token is the best payment system to support this infrastructure for the foreseeable future. The future is a vibrant ecosystem of many tokens, for which healthcare will need a closed loop payment system in place. The result will be an efficient care cycle management positive feedback loop with significant decreases in billions of dollars currently attributed to healthcare payment fraud [4].

The system also incentives those large organizations with ample server storage to trade tokens with small to medium sized healthcare organizations that will need direct access into the blockchain health network without directly implementing a node. Though, the new healthcare policies provide the potential to incentivize providers to work together to improve care pathways, the current EHR architectures come short of enabling this ability, thus, simply granting or receiving tokens facilitates this process.

Therefore, the value of the tokens are tied to the volume of transactions executed in the network. As the Patientory network consistently increases in token transactions the demand for the token increases, resulting in increased value.

Figure 4: Patientory Token Value as a Function of Transactions

3.7 Token Acquisition

PTOY can be acquired through Patientory's native app, crypto-currency market and from another patient, physician or insurer via transfer. Platform users will have the ability to acquire PTOY by sending Ether ("ETH") to the PTOY creation contract on the blockchain during a pre-sale. The Patientory interface will integrate third party trading solutions such as Shapeshift and Coinbase for users who do not have ETH.

The Patientory Token initial distribution will be in the form of a presale. Anyone will be able to acquire PTOY at a discount rate by pledging ETH into the token sale smart contract. Those with other cryptocurrencies such as ETC or BTC can create PTOY via a third-party conversion service that will be available on the pre-sale page.

The founding team will receive a 10% allocation of PTOY, subject to a twelve month holding period. These tokens will serve as longterm incentive for the Patientory founding team. An additional 20% will be allocated to the Patientory Foundation fund to be used for research and development regarding blockchain technology for healthcare use cases.

3.8 Smart Contracts and Insurance claim processing

A. Auto-adjudication

The complexity of medical billing and the third-party reimbursement processes for patients often leads to confusion or misunderstanding between patient, medical provider, and insurer. These complications lead some consumers to be unaware of when, to whom, or for what amount they owe a medical bill or even whether payment was their responsibility or the insurance provider.

Patientory is a platform engineered to leverage both Ethereum blockchain technologies and Fast Healthcare Interoperability Resources (FHIR) compliant application program interfaces (APIs) to increase efficiencies, enable near real-time claim adjudication, provide transparent agreements between stakeholders and decrease fraud.

FHIR was created as an industry standard to format data thereby reducing integration complexity for healthcare and insurance legacy systems. A key aspect to our solution, due to the cost of adding data to the blockchain, is limiting that data to only what is needed for the smart contracts to execute.

With Billing and Insurance Related costs expected to reach 315 Billion dollars (USD) in 2018 and medical offices spending 3.8 hours each week interacting with payers, our platform can bring substantial relief to these operational costs.

Methods that may be employed for the analysis of cross correlation for diagnostic information may also be used to analyze claim data for fraudulent activity. This analysis may also reveal actions such as drug seeking behavior due to the instance of multiple claims. Both of these use cases add value propositions for the use of this system by insurance companies, but the ultimate benefit is beyond this information.

Due to the rule based system that is enforced by the smart contract system, entire coverage agreements may be encoded to smart contracts that are referenced against end users. This would allow for a medical facility to query the system to verify the existence of coverage prior to service delivery. The use of the system to host cost information also allows for the automatic billing between institutions and individuals as token based debt. Thus an institution and an individual may be readily knowledgeable of costs as they are incurred. This removes workload from accounting departments, thus additional value to system adoption.

For this reason Patientory is a closed loop payment system. It is expected that cross chain linking may even allow for the secure exchange of value through the public Ethereum Blockchain. This mechanism is already solved for the arbitration of Bitcoin transactions, although it does require a trusted entity to act as an Oracle.

B. Feasibility

Through the use of existing mechanisms, this architecture may be readily constructed. One such example would be the linking of Amazon Web Service's HIPAA compliant data storage system with the readily deployable ErisDB. This SAAS enables rapid deployment of an Ethereum smart contract capable blockchain with fully permissioned access controls such as those mentioned above. The addition of the passive nodes would need to be constructed, but this is a minimal development cost compared to the development of the complete architecture.

With Patientory's three-tiered Smart Contract architecture, only a subset of the features of a smart contract are implemented on the Ethereum blockchain. Complex business logic is removed from the execution path, which allows the data tier to be optimized to reflect the distributed nature of the network.

The components of the smart contract package implemented on the Ethereum blockchain are the database schema, validation and verification of transactions that append to the ledger, and query optimization logic for reading the ledger.

The business logic is pulled up above the Ethereum blockchain to a separate middle (business) layer. This logic code accesses a variety of services, including secure execution, attestation, identity, cryptographic support, data formatting, reliable messaging, triggers, and the ability to bind that code to schema in specific smart contracts on any number of blockchains, allowing Patientory to plug and play into various healthcare consortiums. These services are provided in a fabric, where the individual pieces of code that support the smart contracts can execute, send transactions to blockchain nodes, and be bound to the schema in the data tier.

3.9 Additional Unique Benefits

Although a medical institution, such as a hospital should not have access to any records that have not been specifically approved, by having users pre-authorize the sharing of information under emergency circumstances, the end user could derive additional benefit from participation in the service. With this in mind, the need of a medical facility to access the records of an unresponsive person in an emergency constitutes a situation that merits privilege escalation given the user has previously authorized this access. In the event that a person is unresponsive, and has their cell phone present, the institution may prove possession of an individual's device by using a secondary signature method that is available from the lock screen of a smart-phone. This second key must not be the same private key as the primary account. Thus, if an institution account submits a request to the blockchain containing the public key of an individual and the smart-phone of that individual has submitted an emergency signature, the blockchain may escalate privilege to allow access to medical records it would not otherwise have access to. **This private key should be considered burnable and be replaced by the individual as soon as possible. In this manner, the secure exchange of information between an individual and an authorized institution may be facilitated in emergency conditions.**

Should an institution request this information without appropriate authorization, the individual would be notified of the actions. If the individual denies this request within a threshold interval, the data is not shared. Further, if an institution attempts multiple fraudulent requests, the institution may be punished by revocation of privilege, monetary punishment, and/or legal actions. The damage caused by losing a cellular device is minimal due to the need for both a cellular device and an institution level key. In the foreseeable future, all insurance cards could be embedded with cryptographic micro-controllers, such as modern credit cards possess, that would facilitate the same operation independent of a smart phone.

4 National/International Health-care Priorities

4.1 Personalized Care

To achieve effective superior care, a person centric approach is important. Such an approach should take into account not only the clinical aspects but the social and economic factors that impede one's ability to successfully engage in care compliance and healthy living to yield sustained wellness.

To yield effective care outcomes requires clearly identifying the barriers of individual health and life situations. With the growing number of patients having 2+ co-morbidities, the “siloed” one-type of care fits-all care delivery approach is not conducive in motivating and addressing effective care outcomes. Hence a more flexible care model tailored to include patients' multi-faceted health and wellness needs has to be considered. This requires that a comprehensive, dynamic interactive care plan in which the patient can actively track, manage, and participate in the individual's care is vital.

4.2 Clinical Outcomes

Patient-related outcome measures (PROMs), which focus on outcomes that are directly related to the patient, have taken on added importance and significance over the past several years. This is due, in part, to the increased attention focused on the patient experience of care and to provide a patient-focused assessment on the burden and impact of disease. PROMs can include symptoms and other aspects of health –related quality of life indicators such as physical or social function, treatment adherence, and satisfaction with treatment. They can also facilitate more accurate patient-physician communication in terms of the burden of treatment-related morbidities by providing a more detailed and complete evaluation of treatments for specific conditions, such as cancer or multiple sclerosis.

PROMs are distinct from traditional clinical efficacy measures (e.g., survival in cancer, smoking cessation) because they directly reflect the impact of disease and its treatment from the patient's perspective. These measures can examine the balance between the efficiency of the treatment and its burden on the patient. It is also effective in looking at areas such as physical functioning and overall well-being, and highlighting the efficacy and safety of treatments in relation to its overall clinical benefit. Because the measures themselves are developed from the patient's perspective, it can also facilitate greater patient involvement in treatment decision-making as well as providing guidance for health care decisions. Essentially, reinforcing a blockchain PROM infrastructure reinforces the ability to incentivize providers and payors in meeting care standards.

5 Conclusion

Blockchain will play an increasingly significant role in healthcare IT and bring beneficial disruption and new efficiencies to every stakeholder in the ecosystem. It is vitally important that healthcare organizations understand the core of blockchain technology to ensure they are ready for the changes the technology entails.

The result will be a new generation of powerful, blockchain-based applications that will shape the next era of business in healthcare. For blockchain to fulfill its potential in healthcare, it must be based on standards to assure the compatibility and interoperability within the siloed health care system landscape.

www.patientory.com
Google Slack Twitter Facebook Reddit BitcoinTalk GitHub Telegram Medium

References

[1] "A Begoyan. An overview of interoperability standards for electronic health records." In: (2007.).

[2] Charles N Mead et al. "Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still dicult. do we really need a better mousetrap?" In: (2006.).

[3] Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. "MedRec". In: (2016). URL: www.pubpub.org/pub/medrec.[Accessed:05-Apr-2017].

[4] National Healthcare Ant-Fraud Association. "The Challenge of Health Care Fraud". In: (). URL: https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

[5] Vitalik Buterin. "A next-generation smart contract and decentralized application platform. White Paper". In: (2014.).

[6] Yan-Cheng Chang and Michael Mitzenmacher. "Privacy preserving keyword searches on remote encrypted data.In International Conference on Applied Cryptography and Network Security". In: ().

[7] Mayo Clinic. "Changes in Burnout and Satisfaction With Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014". In: (). URL: www.mayoclinicproceedings.org.

[8] Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. "Reidao: Digitising Real Estate Ownership". In: (). URL: http://reidao.io/whitepaper.pdf.

[9] et al. Centers for Disease Control Prevention. "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services." In: (2003.).

[10] Roy Thomas Fielding. "Architectural styles and the design of network-based software architectures." In: (2000.).

[11] HHS.gov. "H. H. S. O. of the Secretary Summary of the HIPAA Privacy Rule". In: (2013). URL: www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.[Accessed:04-Apr-2017].

[12] HHS.gov. "Methods for De-identification of PHI". In: (2015). URL: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected.[Accessed:04-Apr-2017].

[13] Alex Mizrahi Iddo Bentov Charles Lee and Meni Rosenfeld. "Proof of activity: Extending bitcoin's proof of work via proof of stake." In: (2014).

[14] Sunny King and Scott Nadal. "PPCoin: Peer-to-peer crypto-currency with proof-of-stake." In: (2012).

[15] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: (2008).

[16] Stean D Norberhuis. In: ().

[17] Pishing Chiang Philip Chuang Maureen Madden Rainer Winnen-burg Rob McClure Steve Emrick Olivier Bodenreider Duc Nguyen and Ivor DSouza. “The NLM Value Set Authority Center.” In: (2013.).

[18] Amit P Sheth. “Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In Interoperating Geographic Information Systems,” in: (1999.).

[19] Nick Szabo. “Formalizing and securing relationships on public networks.” In: (1997.).

[20] “US GPO. CFRx 164 security and privacy. 2008.” In: (). URL: http://www.access.gpo.gov/nara/cfr/waisidx08/45cfr16408.html.Accessed:2016-08-06..