Patientory: una Rete Sanitaria Peer-to-Peer per l'immagazzinamento delle Cartelle Cliniche Elettroniche (EMR) v1.1

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

Maggio 2017

Questo documento è solo a scopi informativi e non costituisce un'offerta o una sollecitazione a vendere quote o securities in Patientory o compagnie collegate o associate. Ogni offerta di tale tipo sarà fatta solo mediante memorandum d'offerta confidenziali e in accordo con i termini di tutte le securities applicabili, nonché con le altre leggi.

Abstract

Da un sito di scambio (exchange) delle informazioni sanitarie (HIE) alimentato dalla blockchain può scaturire il vero valore dell'interoperabilità e della sicurezza informatica. In considerazione della gestione della salute della popolazione, questo sistema ha il potenziale per eliminare la frizione e i costi degli attuali intermediari di terze parti. I propositi sono quelli di una migliorata integrità dei dati, costi di transazione ridotti, decentralizzazione e disintermediazione della fiducia. Essere in grado di coordinare la cura del paziente tramilte un HIE blockchain alleggerisce da servizi non indispensabili ed esami doppione, al tempo stesso abbassando i costi e migliorando l'efficienza del ciclo continuo di assistenza sanitaria, senza infrangere le regole e gli standard dell'HIPAA. Un protocollo sostenuto dalla blockchain e incentrato sui pazienti, Patientory sta cambiando il modo in cui gli i medici curanti gestiscono i dati sanitari e interagiscono con le equipe sanitarie.

Introduzione

Cos'è la Blockchain?

Si tratta della tecnologia alla base della valuta digitale bitcoin; la nascita della blockchain risale ad un individuo (o gruppo) non identificato con lo pseudonimo Satoshi Nakamoto. Dal 2009 la blockchain si è ritagliata un ampio uso nell'industria finanziaria, con l'entrata nel mercato di una varietà di business e servizi dotati di blockchain. La tecnologia Blockchain è utilizzata per condividere un registro generale (ledger) di transazioni attraverso una rete di imprese senza il controllo di alcuna entità. Il registro distribuito (ledger) rende più semplice creare relazioni commerciali costo-efficienti in cui virtualmente ogni singola cosa con un valore può essere tracciata e scambiata senza la necessità di punti centrali di controllo. La tecnologia mette la privacy e il controllo dei dati nelle mani dell'individuo. La fiducia è l'integrità sono stabiliti senza fare affidamento ad intermediari di terze parti.

Infrastruttura dell'Assistenza Sanitaria attuale

Il riallineamento dal concentrarsi sulla “procedura” ad un'”assistenza olistica dell'individuo” richiede che i medici formino “reti” che lavorano insieme per l'obiettivo comune di migliorare l'esito delle cure, per episodi acuti post-cure o tra una cura e l'altra. Il bisogno di cooperazione tra medici curanti che comprendono specialisti, medici generici, infermieri e assistenti sanitari (come nutrizionisti e infermieri addetti alla riabilitazione) ha come risultato il crescente affidamento a tecnologie digitali. Benché tali soluzioni abbiano migliorato significativamente il tracciamento e l'efficienza delle cure, hanno anche avuto come conseguenza la formazione di “silos chiusi” di informazioni sanitarie, principalmente sistemi di cartelle cliniche elettroniche (EMR).
Le organizzazioni governative e sanitarie spendono una mole significativa di tempo e di denaro nella costruzione e nella gestione di sistemi d'informazione tradizionali e di piattaforme di scambio dati; con un continuo bisogno di risorse necessarie alla soluzione di problemi, all'aggiornamento dei parametri di settore, all'esecuzione di misure di recupero e di backup, e all'estrazione di informazioni per motivi di registro.
In risposta alla marcia indietro da parte degli ospedali sull'implementazione delle cartelle cliniche elettroniche, leggi federali e programmi di incentivi hanno reso i dati sanitari più accessibili. Ciononostante, la gran parte dei sistemi ospedalieri non possono ancora condividere facilmente i propri dati. Di conseguenza i dottori impiegano più tempo a scrivere che a parlare con i pazienti. Il crollo dei nervi tra I medici è balzato dal 45 al 54 percento tra il 2011 e il 2014 [1].
Benchè esista la nozione di informazione sanitaria “individualizzata” sia sull'aspetto clinico che del benessere, ciò non si è tradotto in piani d'assistenza sanitaria “personalizzati”. Inoltre, nonostante la gran mole di dati, l'ecosistema sanitario nel complesso è incapace di progettare il valore o il rischio al big data tale da aiutare a prevedere futuri episodi di assistenza per un paziente. Perciò le soluzioni attuali intraprese dall'industria della tecnologia per l'assistenza sanitaria hanno avuto come risultato la scelta per i pazienti tra le cure o la frode economica/della privacy. Man mano che il settore crea ulteriori dati, osserviamo una grande espansione del problema. **La natura distribuita, le proprietà, la tecnologia di sicurezza della blockchain possono aiutare a ridurre i costi, aumentare l'efficienza, e fornire un'infrastruttura di sicurezza adeguata.**

1.1 Rapporto Paziente-Curante

Il nuovo paradigma dell'assistenza sanitaria necessita di un'elargizione delle cure efficace ed ottimale ai pazienti, tale da produrre esiti più positivi. Ciò richiede che gli operatori sanitari principali siano in grado di coordinarsi e collaborare con altri operatori coinvolti e con organizzazioni sanitarie ausiliarie quali laboratori e farmacie. Infine, per la riuscita delle procedure è necessario che i registri dei pazienti siano aggiornati e modificati in tempi ragionevoli.

Il software EMR (fascicolo sanitario elettronico) attuale impedisce un rapporto paziente-curante efficace. I portali paziente non sono molto usati da questi ultimi, a causa del carattere chiuso dell'esperienza paziente. Inoltre, il software fornisce solamente una capacità di scambio delle informazioni limitata tra un sistema e l'altro, e solitamente richiede l'apporto di un particolare individuo designato al loro trasferimento. Ciò ha portato ad

una crescente quantità di ritardi nel fornire assistenza tra più organizzazioni e ad un abbassamento della qualità dei servizi d'assistenza forniti al paziente. Poi, poiché gli i medici curanti impieghano una maggiore quantità tempo nella coordinazione dell'assistenza, l'efficacia nel trattamento dei pazienti e il carico di lavoro sono aumentati significativamente; ne è conseguito un impatto controproducente sull'esito delle cure.

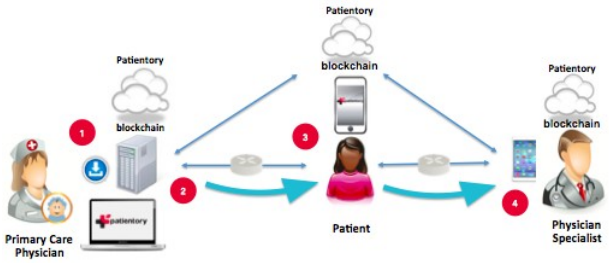

Figure 1: Schema Patientory

In aggiunta, poiché molti dottori non vogliono l'accesso alle EHR da parte dei pazienti, questi ultimi assumono un ruolo passivo nel tracciamento della propria salute. Ciò li porta ad avvertire una mancanza di controllo e possesso della propria salute, sfociando in frustrazione e disimpegno. Benchè ci sia stato recentemente un aumento di app per l'Assistenza Sanitaria Mobile, la novità non si è tradotta in un'assistenza paziente o esiti migliorati, in quanto anch'esse riscontrano le stesse sfide per essere integrate nell'EHR.

Panoramica Sistema

Questi problemi attuali sono risolti attraverso la Rete Blockchain di Patientory. Le EMR (cartelle cliniche elettroniche) del passato sono strutture centralizzate soggette ad hackeraggio, rigide regole di sicurezza, e costi di base ingenti. Con l'implementazione dell'infrastruttura Blockchain di Patientory, gli operatori sanitari vedranno minimizzate le violazioni grazie alle proprietà di controllo accesso inerenti nel sistema; un canale per la facilitata coordinazione dell'assistenza che rende possibile miglioramenti negli esiti di quest'ultima. Qui sopra è presente una descrizione schematica dell'infrastruttura blockchain di Patientory e la sua interoperabilità tra pazienti e i loro medici curanti.

Implementazione Sistema

Linee Guida Norme e Conformità HIPAA

Prima di discutere di implementazioni, è necessario affrontare le restrizioni applicate per ordine dell'Health Insurance Portability and Accountability Act del 1996 (HIPAA). Le norme che ci interessano particolarmente sono la Privacy Rule, Security Rule, e le Linee Guida per il Cloud Computing. L'intento di questo paper non è quello di fare un'investigazione dettagliata della legge HIPAA. Quegli elementi che sono pertinenti alla discussione

sull'implementazione verranno definiti e discussi più in dettaglio nel momento in cui ne concernono l'applicazione.

Privacy Rule (norma sulla Privacy)

Il modello di business di Patientory rende necessaria l'osservanza della Privacy Rule a causa dell'immagazzinamento e trasmissione di informazioni private di assistenza sanitaria. L'applicabilità della privacy rule è sintetizzata come, "La privacy rule...(è applicata) e piani sanitari, camere di compensazione sanitarie, e a qualunque operatore sanitario che trasmetta informazioni sanitarie in forma elettronica" [2]. In aggiunta a questi operatori, le parti che agiscono in loro vece, come fornitori di un servizio, sono anche responsabili per il rispetto dell'HIPAA. Questi operatori di seconda mano sono chiamati Soci d'Affari (BA – Business Associates), e il documento giuridico che descrive regole e norme a cui i BA devono aderire è chiamato Contratto per Soci d'Affari (BAC – Business Associate Contract). L'HIPAA stabilisce requisiti rigidi sulla natura di questi accordi.

I punti di merito, ad un'analisi iniziale, sono quei requisiti che specificano l'autorizzazione all'uso, l'uso d'informazioni de-identificate, e la definizione di informazione privata. L'informazione sanitaria privata (PHI o ePHI per i dati elettronici) è definita come "tutte le informazioni sanitarie identificabili individualmente possedute o trasmesse da un'entità coperta dalla norma o il suo socio d'affari, in qualunque forma o media, sia esso elettronico, cartaceo, oppure orale"[2]. Le informazioni sanitarie de-identificate sono definite come "informazioni sanitarie che non identificano un individuo e nei confronti delle quali non vi è ragione di credere che le informazioni possano essere usate per identificare il suddetto"[2]. [2]. I dati de-identificati usano restrizioni che sono sommate nel modo seguente: "Non ci sono restrizioni sull'uso o la divulgazione di informazioni sanitarie de-identificate. Le informazioni de-identificate nè identificano nè forniscono una ragionevole base per l'identificazione di un individuo"[3]. Il confine tra dato identificabile e de-identificabile è definito come qualunque informazione che possa restringere il possibile numero di individui a cui una serie di informazioni è associata a meno dello 0,04% della popolazione totale degli Stati Uniti.

Security Rule (Norma sulla Sicurezza) e Linee Guida Cloud Computing

A causa della lunghezza dei contenuti collegati a questo argomento, saranno isolati solo gli elementi di interesse principale come riferimento. L'interesse principale è il seguente, "quando un entità coperta dalla norma svolge i servizi di un CSP per creare, ricevere, fare manutenzione di, o trasmettere ePHI (quali il processo e/o l'immagazzinamento di ePHI), su sua vece, il CSP è un socio d'affari sotto l'HIPAA. Inoltre, quando un socio d'affari subappalta con una CSP per creare, ricevere, fare manutenzione di, o trasmettere ePHI su sua vece, il subappaltatore CSP stesso è un socio d'affari. Ciò è vero anche se il CSP elabora o immagazzina solo ePHI criptati e non possiede la chiave di dectrittazione dei dati. La mancanza di una chiave di decrittazione non esenta un CSP dallo stato di socio d'affari e dagli obblighi relativi alle Rule dell'HIPAA. Di conseguenza, l'entità coperta dalle norme (o il socio d'affari) e il CSP devono rientrare in un accordo tra soci d'affari (BAA – business associate agreement) conforme all'HIPAA, e il CSP è contrattualmente responsabile per il rispetto dei termini del BAA e direttamente responsabile per il rispetto dei requisiti applicabili relativi alle Rules dell'HIPAA" [3].

Le entità coperte dalle norme spesso usano fornitori di memoria Cloud (CSP – Cloud Storage Provider) per conservare le informazioni sanitarie, spesso con la motivazione che è più conveniente e i costi di gestione IT sono più contenuti. Tuttavia, affidandosi a fornitori cloud per la l'immagazzinamento delle informazioni personali, i consumatori cedono il controllo diretto ai dati e di conseguenza non sanno chi vi ha accesso o

dove sono localizzati geograficamente. Anche se un accordo tra socio d'affari esplicito viene sviluppato tra il socio d'affari e il fornitore di memoria cloud, fornirebbe solo i termini sulle responsabilità delle parti per privacy e sicurezza dei dati in caso di un'infrazione di questi ultimi. Il consumatore potrebbe potenzialmente avere il controllo sull'accesso a questi flussi di dati, ma dipenderebbe dal fornitore di memoria cloud per l'applicazione di quei privilegi.

Sebbene l'utilizzo della memoria cloud sia popolare, ci sono ancora un certo numero di rischi che un consumatore intraprende per i propri dati personali nell'utilizzo di questo meccanismo. Nell'architettura basata sul cloud, i dati sono replicati e spostati frequentemente, perciò il rischio di uso non autorizzato dei dati aumenta. In aggiunta, molteplici individui hanno potenziale accesso ai dati, quali amministratori, ingegneri della rete, e tecnici esperti che compiono servizi su, o per, i server che contengono quei dati; nche questo accresce il rischio di accesso e uso non autorizzato. Tuttavia, anche se i dati sono sicuri attraverso rigidi controlli d'accesso e sono criptati al punto di origine e durante il transito, rappresenta comunque un problema per lo sviluppo di Misure di Esiti Registrati dai Pazienti (PROM – Patient-Reported Outcomes Measures). Il concetto di PROM è quello di sviluppare misure incentrate sul paziente relativamente ad un'area che interessa particolarmente il suddetto, nonché in cui il coinvolgimento e i suggerimenti sono essenziali per la loro riuscita implementazione. L'accesso a larghi flussi di dati da una varietà di dispositivi che sono parte della rete dell'Internet delle Cose, come sono usati adesso, in congiunzione con servizi basati sul cloud, possono fornire una base sulla quale fondare un PROM, ma è difficile sapere se i dati chiusi nel cloud produrranno misure misure che avranno il significato e la rilevanza voluti per un paziente.

L'implementazione di tecnologia blockchain per garantire e potenziare la sicurezza dati per tutti i registri medici associati al sistema può minimizzare le violazioni sanitarie ed ultimare la decentralizzazione della proprietà dei registri. Verrà utilizzato il processo di criptazione dei dati usando diversi algoritmi quando questi sono inviati al database, e saranno decriptati al loro recupero. Durante la trasmissione e il recupero, i dati saranno criptati utilizzando algoritmi che rispettano il NIST, come stabilito dalla legge. Quindi, tutti gli scambi di informazioni rispetteranno le prassi migliori delineate nelle specifiche del NIST.

Riguardo alla rapida crescita nel numero di violazioni dei dati affrontate dall'industria dell'assistenza sanitaria, la tecnologia blockchain rede la conformità all'HIPAA praticabile sia per pazienti che per medici curanti.

1.A. Analisi Sistema Blockchain delle Limitazioni dovute alle Restrizioni HIPAA

La blockchain di Ethereum facilita un diverso sottoinsieme di implementazioni per mezzo dell'applicazione di un liguaggio di programmazione touring-completo che è eseguito sulla Macchina Virtuale Ethereum. Questi sistemi hanno limitazioni poiché la macchina virtuale non presenta l'ispezione esterna più ampia di Internet se non attraverso l'uso di Servizi Oracolo (Oracle). In aggiunta, le limitazioni di memoria della blockchain sono preservate dal costo del gas per la memoria e il costo del gas per l'accesso ai dati. Al momento della scrittura di questo paper, il tempo di blocco della catena (blockchain) stabilisce un limite per le richieste di modifica di stato di almeno quindici secondi.

La limitazione nel contenere informazioni private della blockchain potrebbe essere superato attraverso offuscazione dati, quali la criptazione, ma nell'eventualità che la chiave di decrittazione venga svelata, non c'è alcun modo di rimuovere quei dati sensibili dalla blockchain. In considerazione del fatto che l'obiettivo è quello di avere dati conformi all'HIPAA, ciò potrebbe potenzialmente risultare in una persistente, irreparabile fuga di informazioni a causa dell'immutabilità della blockchain stessa. Benchè i dati de-identificati possano in teoria essere immagazzinati sulla Blockchain pubblica di Ethereum, sarebbe disastroso presumere che il

meccanismo di filtraggio de-identificativo non fallirà mai, o che le informazioni a banda laterale associate alle interazioni della blockchain non possano rivelare inavvertitamente l'identità. Questa conclusione è stata raggiunta anche dall'MIT Media Lab durante la formazione dei protocolli MedRec e riassunti nel whitepaper MedRec [3]. Recuperare l'informazione a banda laterale potrebbe essere tanto semplice quanto osservare timbri orari e interazioni con noti contratti d'immagazzinamento dati.

Attraverso quest'analisi potrebbe essere possibile associare un individuo con un'istituzione, e cosa ancora più importante con il tempo durante il quale era presente in una struttura. Data la natura specializzata di alcune strutture, una tale informazione è sufficiente a costituire una violazione dell'HIPAA a causa dell'abilità di un osservatore passivo di dedurre identità, posizione, tempo d'interazione, e verosimilmente classe della diagnosi.

Data la natura remota di un tale posizionamento, la riduzione a meno dello 0,04% della popolazione diventa banale. Questi fatti costituiscono punti deboli irragionevoli che devono essere riconosciuti. Inoltre, l'immagazzinamento diretto di informazioni anche criptate rende il gestore del database responsabile per la creazione di una BAC a causa del suo agire come struttura di conservazione dati (Guarda la sezione intitolata “Security Rule e Linee Guida Cloud Computing). Queste sono aspettative irragionevoli poiché ogni miner, anche quegli individui che mantengono nodi passivi, rientrerebbero tutti nell'HIPAA. A causa di queste preoccupazioni, abbiamo implementato un meccanismo di conservazione persistente di informazioni sensibili attraverso l'uso di un'implementazione privata di una blockchain basata su Ethereum.

Obiettivi d'Implementazione per Usabilità e Sicurezza

Gli obiettivi principali di qualunque sistema sicuro possono riassumersi com gli obiettivi alla riservatezza, integrità, disponibilità, responsabilità e garanzia delle informazioni/identità. Per raggiungere questi obiettivi devono essere definiti aggressore e utente. A ognuno di questi ruoli e necessario riconoscere abilità specifiche. Dal punto di vista dell'utente, il sistema deve essere sufficientemente trasparente in modo che non sia necessaria alcuna conoscenza avanzata. Inoltre, a causa dell'inabilità dell'utente comune di fare complesse considerazioni che riguardano la sicurezza informatica, il processo deve essere resistente alle azioni dell'utente stesso.

Nell'evenienza che avvenga un attacco, il sistema è creato in modo tale che la quantità di impegno necessaria a compromettere una risorsa valga più della della risorsa stessa. Ciò è dovuto alla consapevolezza che qualcuno sufficientemente all'avanguardia, con risorse, tempo e impegno adeguati potrà sempre violare qualunque sistema. In sintesi, non esiste difesa perfetta. Tenendo bene a mente queste restrizioni, l'implementazione può essere discussa al fine di raggiungere gli obiettivi menzionati in precedenza.

Definizione dell'Implementazione Hardware e Rete

Per soddisfare gli obiettivi di progettazione affermati più sopra, l'implementazione di sistema selezionata richiede diversi sistemi indipendenti. Ogni sistema suddivide autorità, garantisce che solo le entità autorizzate possano interagire in maniera approvata, e fornisce un meccanismo per l'incremento della sicurezza preservando allo stesso tempo la disponibilità. Questo sistema è stato anche progettato in modo che la scalabilità (scaling) possa essere raggiunta mediante schemi di chiamata gerarchici (calling schemes). Questi sistemi sono descritti in modo completo più sotto.

L'entità rivolta al pubblico è un Server Procedura di Chiamata Remota (RPC) che funge da interfaccia per un'implementazione privata della Blockchain di Ethereum (blockchain autorizzata(permissioned)). Questa

rete di nodi blockchain è solo autorizzata a interagire con gli altri nodi della blockchain, una chiave di autorizzazione entità, la struttura di immagazzinamento conforme all'HIPAA, e il Server RPC. La chiave di autorizzazione entità è la risorsa che genera coppie di chiavi pubbliche/private per l'uso sulla blockchain. La struttura di immagazzinamento conforme all'HIPAA conserva i dati effettivi che costituiscono le informazione sanitarie elettroniche private (ePHI).

Quando avviene una richiesta per dei dati, il sistema conforme all'HIPAA può essere autorizzato a parlare con l'inoltratore, che poi reindirizza i dati verso il server RPC. In alternativa, potrebbe essere strutturato in modo che il magazzino dati HIPAA parli direttamente al server RPC. Ogni implementazione ha dei vantaggi che devono essere considerati prima della selezione finale. In uno qualunque dei casi, la struttura di immagazzinamento HIPAA decripta le porzioni significative del database su richiesta. Queste informazioni decriptate sono poi ricriptate usando la chiave pubblica del richiedente per la trasmissione. Questa chiave pubblica è anche la chiave pubblica del contratto che funge da interfaccia di controllo dalla blockchain ai dati HIPAA.
Il diagramma della topologia di rete specificata è visualizzato nella figura 2.

Definizione dell'Implementazione Software

In aggiunta all'isolazione fisica di sistemi nell'implementazione hardware e rete, il controllo all'accesso del software facilita l'integrità dei dati e

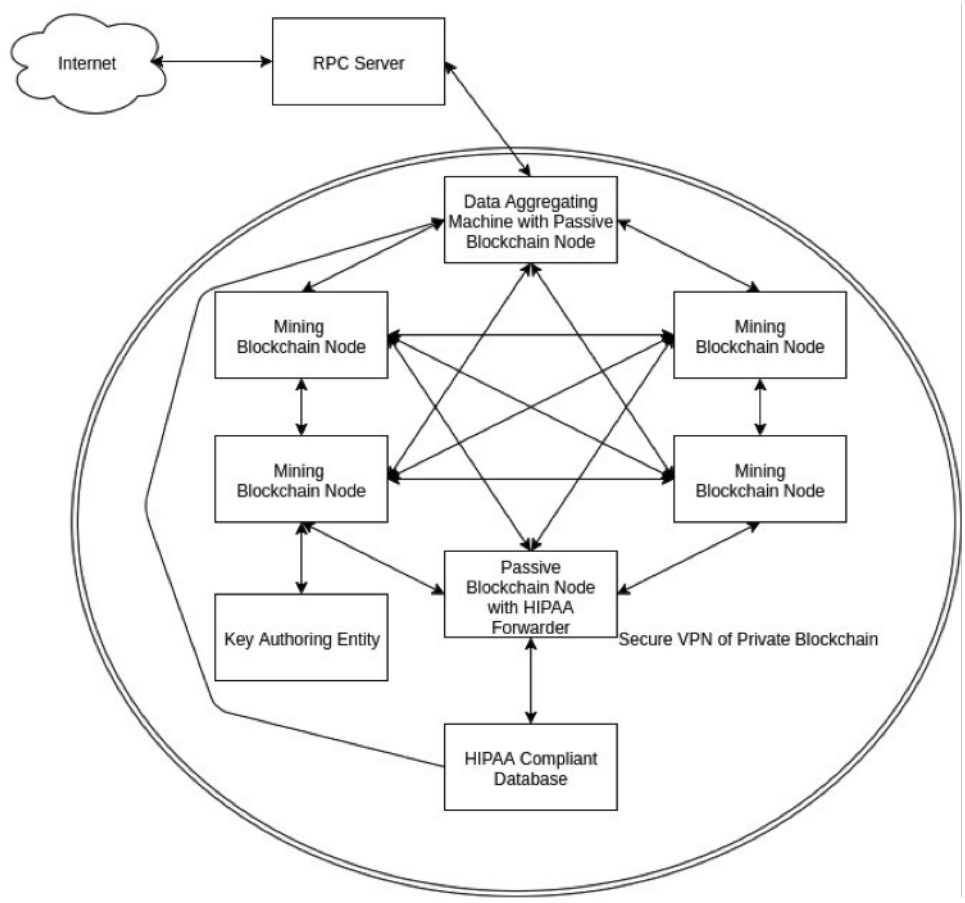

Figure 2: Topografia Rete Blockchain Patientory

la verifica dell'autorizzazione per le entità richiedenti. Il sistema software dalla prospettiva del controllo all'accesso e della criptazione dei dati è descritta più sotto.

Il database conforme all'HIPAA accetterà solamente connessioni dalle connessioni limitate (inbound) dall'inoltratore HIPAA. Ciò garantisce che il flusso del traffico sia isolato da percorsi notoriamente controllati. L'inoltratore HIPAA agirà solamente per inviare una richiesta alla struttura d'immagazzinamento HIPAA in attesa che una transazione valida sia compiuta sulla blockchain, e questa transazione è risultata nell'emissione di un evento che invoca una richiesta. L'evento che invoca una richiesta deve contenere la chiave pubblica del richiedente, e i campi di dati che sono richiesti. Infine, il server RPC usa un'API con accesso controllato che permette solo ad utenti registrati di interagire con il server.

Per capire la gerarchia chiamate del sistema, bisogna prima descrivere la struttura del contratto per facilitare l'accesso. Ogni utente del sistema è associato ad un indirizzo privato sulla blockchain privata. Ogni indirizzo privato è autorizzato a parlare direttamente solo ad un contratto sulla blockchain. Questo contratto è il contratto di classe dell'individuo. Istituzioni, impiegati di istituzioni, e clienti sono oggetti di livello classe.

Questi oggetti di livello classe sono interfaccie basate su permessi. Il Contratto Istituzione ha una lista di tutti i clienti che hanno concesso privilegi di visualizzazione all'istituzione, e ogni Contratto Cliente ha una lista di tutte le istituzioni alle quali ha dato permessi. Il contratto detenuto dall'istituzione ha funzioni che facilitano la recova dei permessi concessi all'istituzione da parte dell'utente. **Il Contratto Istituzione non può modificare autonomamente questa lista, prevenendo così l'accesso non autorizzato ai registri degli individui.** In Aggiunta, il Contratto Istituzione possiede una lista di impiegati autorizzati per il cui mantenimento è completamente accessoriato. Questo schema di permessi dovrebbe idealmente funzionare in modo tale che la revoca di un permesso è effettuata ad intervalli semi-regolari per impedire che un'istituzione conservi inavvertitaemente i diritti d'accesso di un ex impiegato.

All'interno di questo sistema, tutti gli individui esterni devono interagire attraverso l'invio di transazioni firmate che cifrano la chiamata di richiesta. Queste transazioni sono inviate attraverso il server RPC non appena convalidate dell'utente. Il server RPC trasmette queste richieste al server di aggregazione dati che poi le inoltra ai miner in base al meccanismo di condivisione del carico. I miner poi processano la richiesta inviando la transazione al contratto di controllo della rispettiva parte, per conto dell'individuo che effettua la chiamata. Questo contratto contiene i permessi dei

dati interni al contratto ai quali l'entità è autorizzata ad accedere. Questo contratto è la sola entità che accetterà una transazione da una richiesta esterna. Così si stabilisce un meccanismo volto a controllare in pieno le operazioni sulla blockchain.

Per ogni data transazione, viene creata una voce di registro immutabile dell'invididuo che effettua la chiamata. Ciò garantisce che tutti i tentativi di accesso alle informazioni siano registrati. I dati effettivi conservati nel contratto utente sono un sistema di puntatori di hash che quando sono risolti dal server di memoria HIPAA restituiscono i dati giusti. Queste informazioni passano all'inoltratore HIPAA mediante l'esecuzione di una richiesta di transazione valida. Il meccanismo che facilita questa comunicazione è indiretto e si manifesta attraverso il sistema di notifica eventi della blockchain. A causa delle limitazioni per cui il richiedente può solo comunicare con il database mediante transazioni valide, e per cui l'utente non può modificare direttamente le informazioni proprie, il controllo all'accesso è dimostrabile. Dalla prospettiva delle istituzioni, i meccanismi sono simili, eccetto che il contratto istituzione ospita una lista di utenti da cui può richiedere dati e una lista di utenti che possono interagire con questa istituzione in quanto dipendenti. Quando una richiesta di transazione ha origine dal contratto del dipendente di un'istituzione, il contratto di controllo chiama il contratto istituzione, che a sua volta chiama il contratto utente per richiedere i puntatori dei dati che risolvono ePHI. In attesa che l'istituzione sia sulla lista delle istituzioni approvate per l'utente, il contratto restituisce i puntatori hash appropriati. Questi puntatori sono poi pubblicati come nota evento che nuovamente arriva alla struttura d'immagazzinamento HIPAA.

Per chiarezza, il processo totale di una singola richiesta è il seguente: la parte esterna richiede i dati dal servizio contattando il server RPC con una transazione firmata crittograficamente da inviare alla blockchain. Il server RPC verifica l'identità della parte esterna mediante la firma o la richiesta di accesso.

In attesa che la firma coincida con una voce nel database delle chiavi pubbliche dotate di permesso, il server RPC accetta la richiesta e la invia alla Macchina di Aggregazione Dati (Data Aggregate Machine). La Macchina di Aggregazione Dati invia poi le richieste ai verificatori della blockchain privata. I verificatori ricevono la richiesta come chiamata da un conto della blockchain verso un contratto bersaglio. Questa transazione causa anche l'emissione di un una nota evento sulla blockchain. Questa nota evento è osservata dal mittente HIPAA, che si aziona creando una richiesta criptata contro la memoria HIPAA basata sulle hash della nota evento. Questo messaggio contiene anche la chiave pubblica della parte richiedente. Il sistema di database conforme all'HIPAA osserva questa richiesta e trasmette una copia criptata dell'informazione al server RPC usando la chiave pubblica della parte richiedente. Il server RPC restituisce poi questa informazione alla parte richiedente riassociando l'IP richiedente alla chiave pubblica nel messaggio. Il server RPC trasmette questo messaggio senza mai aver visto I dati sottostanti. Questi dati sono poi immediatamente distrutti dal server RPC, garantendo così che il server RPC agisca da tramite non necessità di essere conforme all'HIPAA.

Il meccanismo di pubblicazione dati è anch'esso di natura simile, ma I dati che sono invitati sono criptati con la chiave pubblica della struttura d'immagazzinamento HIPAA: Le altre operazioni sono identica ad eccezione dei dati che sono inviati e passano attraverso il sistema di nota evento. Così, a causa della bassa collisione delle funzioni hashing e le nonce marcate orariamente, i dati possono essere conservati con un contratto in grado di elaborare l'indirizzo in cui i dati inviati sono posizionati all'interno della struttura d'immagazzinamento HIPAA.

Infine, analizziamo la distribuzione alle entità delle chiavi private . Ciò potrebbe essere facilitato attraverso mezzi visivi per gli utenti smartphone, in modo analogo all'uso dei codici QR come indirizzi Ethereum. In alternativa tramiti possono anche essere stabiliti utilizzando applicazioni sia su computer desktop che su dispositivi tablet/smartphone. La perdita di una chiave non è un evento catastrofico, per via dell'abilità di rimuovere con permessi amministratore il controllo all'accesso di un contratto da una chiave e passarlo ad un'altra chiave.

Interoperabilità

I sistemi EHR sono basati su un'architettura di convalida credentiali isolata in cui i dati dei pazienti sono tenuti in ugnuno dei sistemi separati. La conseguenza di ciò sono soluzioni software “add-on” di coordinazione assistenza diversi uno ad uno per ogni sistema, in modo da permettere la coordinazione delle cure con altri medici e organizzazioni sanitarie supplementarie. Tuttavia, l'accesso alle informazioni dall'organizzazione Sanitaria principale alle altre organizzazioni avviene solo in capacità limitate quali Lettura, Entrata, Invio o Notifica. Inoltre, il Paziente/Consumatore ha un'interazione o un coinvolgimento molto limitati in questo scambio di informazioni. In aggiunta, un iconveniente nei meccanismi di scambio dati esistenti è la rettifica degli errori che si verificano durante il processo di invio.

Una volta che la blockchain e il suo contratto intelligente sono configurati, i parametri diventano assoluti. Il paziente diventa l'intermediario primario nell'invio e nella ricezione delle informazioni mediche, rendendo inutili aggiornamenti frequenti e la risoluzione problemi del software. Poiché I registri della blockchain sono anche immutabili e conservati tra tutti gli utenti partecipanti, non sono necessari casi di recoupero. Per di più, la struttura trasparente di informazioni della blockchain potrebbe abolire molti punti d'integrazione dello

scambio dati e molte lunghe attività di resoconto attività.

Processi e Scalabilità

Gli utenti hanno il controllo di tutte le loro informazioni e trasferimenti, garantendo così alta qualità dei dati che sono completi, consistenti, tempestivi, accurati, e ampiamente disponibili, rendendoli durevoli e affidabili. A causa del database decentralizzato, la blockchain non ha un punto critico ed è in grado più facilmente di resistere ad attacchi dolosi.

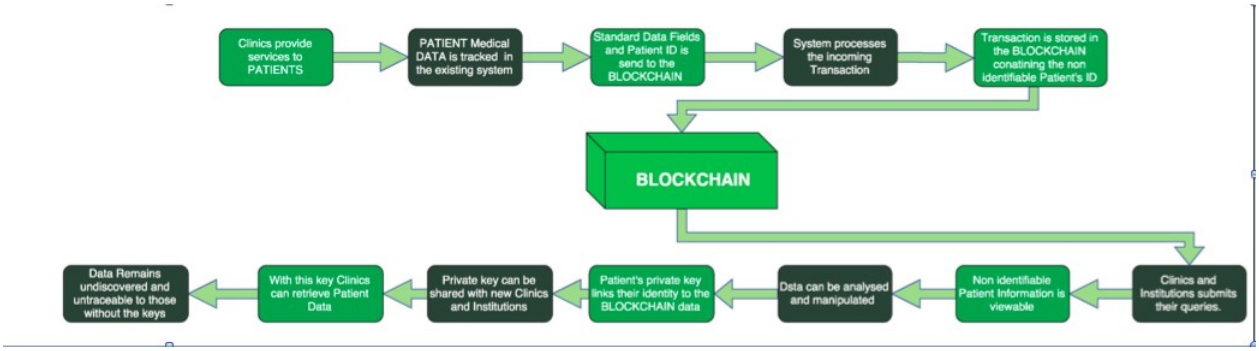

Figure 3: Diagramma Flusso Processi Blockchain

In ogni rete d'Assistenza è necessario garantire che I partecipanti che collaborano insieme possano dipendere l'uno dall'altro per portare a ermine quei servizi che ci si aspetta necessariamente da loro. Per questo motivo, ci deve essere un modo per garantire la responsabilità per I servizi e le mansioni, I quali ci si aspetta vengano portati a termine in tempi brevi, nonché la responsabilità associata ai servizi che non sono compiuti in quei tempi e alla qualità secondo aspettative. Quindi, un'infrastruttura per l'Assistenza Sanitaria deve essere in grado di monitorare senza sforzi le informazioni necessarie affinché il Medico Curante Primario possa valutare la rete dell'Assistenza. Inoltre, man mano che la rete dell'Assistenza cresce e queste interazioni tra medici curanti della rete aumentano, l'infrastruttura sanitaria dovrebbe essere in grado di adattarsi in dimensione.

The key aspect to building a highly scalable and distributed Care

L'aspetto chiave alla costruzione di un sistema di gestione d'assistenza sanitaria scalabile e distribuito è la presenza di un framework peer-to-peer. Un framework tale è già stato utilizzato in una serie di settori industriali quali media, sport, edilizia, ingrosso; la visualizzazione della blockchain può essere facilmente un software aggiuntivo (add-on) che fa da connettore ai framework centralizzati esistenti[7]. Questo ci ha portato ad esplorare l'utilizzo

del framework della blockchain per la sua applicabilità nel supportare la costruzione di un framework peer-to-peer per l'assistenza sanitaria.

La promessa della blockchain è quella di convalidare due o più entità impegnate in una “transazione d'assistenza sanitaria”. Ciò fornisce due attributi chiave rispetto al modello di autenticazione centralizzato. Il primo attributo è che le parti interessate pssono interagire al “livello transazione” del “rapporto di fiducia”. Il secondo attributo è che la finestra delle responsabilità in un tale rapporto è limitata solamente all'interazione al “livello transazione”. Questo è molto utile in quanto limita l'accesso alle informazioni nonhé le responsabilità tra le parti coinvolte e allo stesso tempo permette ad una parte di entrare in un rapporto di transazione con un numero di altri operatori in base alle loro specifiche possibilità e al tipo di assistenza da destinare al paziente. Ciò è un sostanziale miglioramento rispetto ai sistemi centralizzati convenzionali che devono limitare il numero di operatori per un'ampia gamma di bisogni dei pazienti, a causa degli sforzi necessari per gestire l'accesso e le responsabilità.

Sito di Scambio Informazioni Sanitarie e Token

Il token Patientory (PTOY) è la benzina che alimenta l'infrastruttura della blockchain. L'utilizzo primario del token è quello di regolare l'allocazione di memoria del network, le misure di qualità dell'assistenza sanitaria e i cicli di pagamento dei ricavi.

I pazienti ricevono una quantità di spazio specifica gratis per conservare informazioni sulla rete Patientory. I PTOY permettono loro di comprare spazio di memoria extra dai nodi assemblati nei sistemi ospedalieri. PTOY possono essere acquistati tramite la piattaforma o tramite un sito di scambio.

Anche le organizzazioni sanitarie utilizzano PTOY in questo modo. Vengono anche usati nei pagamenti quando vengono eseguiti contratti intelligenti con compagnie d'assicurazione sanitaria e servono da meccanismo per regolare metriche di modello basate sul valore.

Per far sì che che gli Stati Uniti passino con successo dal modello tariffe-per-servizio al modello basato sul valore, è necessaria un'infrastruttura IT di assistenza sanitaria che renda possibile alle organizzazioni connettere qualità, valore ed efficacia degli interventi medici attraverso un modello di retribuzione rispettabile.

La retribuzione sarà basata su quanto efficace è il lavoro comune dei medici curanti, per garantire un miglioramento nella qualità dell'assistenza e degli esiti per la salute, e allo stesso tempo ridurre i costi associati all'assistenza. Per incentivare fortemente alla creazione di migliori regimi d'assistenza i diversi partecipanti alla rete, è stabilita una retribuzione dei risparmi (rimborsi) condivisi basata sul merito. Per allocare efficaciemente una quota proporzionata al medico curante che ha contribuito

maggiormente ai risparmi complessivi, un tracciamento ben definito dei loro contributi è misurabile dai contratti intelligenti sulla rete blockchain.

Un'altro effetto fondamentale del nuovo paradigma di assistenza sanitaria è il modello di retribuzione in cui i medici curanti hanno diritto a ricevere una retribuzione aggiuntiva che vada oltre le cure fornite. Tale retribuzione è il risultato dei risparmi che sono generate in base a quanto efficaciemente i medici gestiscono l'assistenza negli esiti della salute del paziente (incentivi). Tutti i risparmi generati attraverso una gestione efficiente della cura del paziente possono essere trattenuti dai medici e dalla loro rete di partner come parte dell'aspetto risparmi condivisi del nuovo paradigma di assistenza sanitaria.

La nostra proposta dà l'abilità ai paganti di trasferire token come inventivi ai medici che ottengono queste misurazioni qualitative. L'abilità di tracciare e gestire senza intoppi I contratti intelligenti da cui I benefici possono essere facilmente estratti fornisce la “carota” necessaria a medici e pazienti per partecipare attivamente ad una collaborazione simbiotica. Al contrario, se uno o più partecipanti subisce determinate penalità attraverso passività, può incorrere in ____ con altrettanta facilità. Questo approccio “bastone e carota” fornisce la spinta necessaria a trasformare l'industria dell'assistenza sanitaria dalla mentalità della gestione delle malattie a una mentalità della salute nello stile di vita.

D'ora in avanti, i token Patientory emessi (PTOY) sono I token nativi della piattaforma Patientory. In cambio dei token PTOY, gli utenti saranno in grado di usare la rete per affittare spazio d'immagazzinamento delle informazioni sanitarie, e per eseguire pagamenti e transazioni di contratti intelligenti destinati specificatamente al settore sanitario.

Crediamo fermamente che usare il token sia il sistema di pagamento migliore per sostenere quest'infrastruttura nel futuro prossimo. Il futuro è un vibrante ecosistema di molti token, per i quali la sanità avrà bisogno della messa in piedi di un sistema chiuso di pagamento circolare. Il risultato sarà un efficiente circuito di suggerimenti positivi sulla gestione del circuito di assistenza con diminuzioni significative nei miliardi in frode attualmente attribuiti ai pagamenti nel settore sanitario[4].

Il sistema incentiva anche grandi organizzazzioni con ampi server di memoria a scambiare token con le organizzazioni d'assistenza sanitaria piccole e medie, che avranno bisogno dell'accesso diretto alla rete blockchain sanitaria senza implementare un nodo. Sebbene le nuove politiche di assistenza sanitaria forniscano il potenziale per incentivare i medici a lavorare insieme per migliorare gli andamenti delle cure, le attuali architetture EHR risultano insufficienti a questo fine, perciò il processo viene facilitato dalla semplice elargizione o ricezione di token.

Il valore dei token è quindi legato al volume delle transazioni eseguite nella rete. Man mano che il volume delle transazioni nella rete Patientory cresce, così cresce la domanda per il token, portandolo ad un valore più alto.

Figure 4: Valore del Token Patientory come Funzione delle Transazioni

Acquisizione Token

PTOY può essere acquistato attraverso l'app nativa di Patientory, dal mercato delle criptovalute o da un altro paziente, dottore o assicuratore via trasferimento. Gli utenti della piattaforma avranno l'abilità di acquisire PTOY inviando Ether (“ETH”) al contratto di creazione PTOY sulla blockchain durante la prevendita. L'interfaccia Patientory integrerà soluzioni di trading di terze parti quali Schapeshift e Coinbase per gli utenti che non possiedono ETH.

La distribuzione iniziale del token Patientory sarà in forma di prevendita. Chiunque sarà in grado di acquistare PTOY a prezzo scontato inviando ETH al contratto intelligente di vendita. Coloro che hanno altre criptovalute quali ETC o BTC possono creare PTOY mediante un servizio di conversione di terze parti che sarà disponibile alla pagina della prevendita.

Il team fondante riceverà il 10% dei PTOY, che saranno soggetti ad un periodo di inaccessibilità di 12 mesi. Questi token serviranno da incentivo a lungo termine per il team di Patientory. Un 20% aggiuntivo sarà allocato al fondo della Fondazione Patientory da usarsi per la ricerca e lo sviluppo della tecnologia blockchain in casi d'uso nel settore sanitario.

Contratti Intelligenti e Processamento Reclami Assicurativi

Auto-aggiudicazione

La complessità della fatturazione medica e i processi per pazienti di rimborso di terze parti portano spesso a confuzione e malintesi tra paziente, fornitore di cure mediche, e assicuratore. Tali compliczioni portano alcuni consumatori a non essere consci di quando, a chi, e a quanto ammontino le proprie spese mediche, o persino se il pagamento spetti a loro o alla propria assicurazione.

Patientory è una piattaforma progettata per sfruttare le tecnologie della blockchain Ethereum e API conformi alle Risorse di Veloce Interoperabilità per l'Assistenza Sanitaria (FHIR) per incrementare l'efficienza, favorire l'aggiudcazione dei reclami in tempo reale, fornire accordi trasparenti tra stakeholder e diminuire le frodi.

FHIR è stato creato come standard del settore per disporre I dati portando così a ridurre la complessità nell'integrazione dei sistemi assicurativi e d'assistenza sanitaria. Un aspetto chiave della nostra soluzione, a causa del costo dell'aggiunta dei dati alla

blockchain, è la limitazione per cui vengono aggiunti solo i dati necessari all'esecuzione del contratto intelligente.

Considerati i costi relativi a Fatturazione e Assicurazione, che si prevede raggiungano i 315 miliardi di dollari nel 2018 e considerate le 3,8 ore di interazione tra gli uffici medici e i paganti, la nostra piattaforma può portare un sollievo considerevole a questi costi operativi.

I metodi che possono essere utilizzati per l'analisi di correlazione incrociata nelle informazioni diagnostiche possono anche essere utilizzati per analizzare i dati sui reclami in cerca di attività fraudolente. Tale analisi può anche rivelare azioni quali i comportamenti volti alla ricerca deliberata di sostanze in base alla presenza di molteplici richieste. Entrambi i casi d'uso aggiungono valore alla proposta per l'uso di questi sistemi in compagnie d'assicurazione, ma il vantaggio maggiore va oltre queste informazioni.

Per via del sistema basato su regole applicato dal sistema del contratto intelligente, interi accordi di copertura possono essere programmati in contratti intelligenti che si riferiscono ad utenti finali. Ciò permetterebbe ad una struttura medica di richiedere al sistema di verificare l'esistenza di copertura prima dell'elargizione di un servizio. L'uso del sistema per contenere le informazioni sui costi permette anche la fatturazione automatica tra istituzioni e individui come debito basato su token. Così un'istituzione e un individuo possono essere preventivamente preparati ai costi da loro sostenuti. Ciò rimuove carico di lavoro dai dipartimenti contabili, aggiungendo valore all'adozione del sistema.

Per questa ragione Patientory è un sistema di pagamento a circuito chiuso. Si prevede che il collegamento inter-chain possa persino permettere lo scambio sicuro di valore attraverso la Blockchain pubblica di Ethereum. Questo meccanismo è già risolto per la mediazione delle transazioni in Bitcoin, anche se necessita di un entità fidata che funga da Oracolo. For this reason Patientory is a closed loop payment system.

A. Praticabilità

Attraverso l'uso di meccanismi esistenti, questa architettura può essere prontamente costruita. Un esempio di questo tipo è il collegamento di sistemi di immagazzinamento dati Amazon Service conformi all'HIPAA con ErisDB proni all'avvio. Questo SAAS permette il rapido avvio di una blockchain con funzionalità contratto intelligente di Ethereum, che abbia controlli d'accesso con permessi come quelli menzionati più sopra. L'aggiunta di nodi passivi da costruirsi sarebbe necessaria, ma questo è uno sviluppo dal costo minimo rispetto allo sviluppo dell'intera architettura.

Con l'architettura Patientory su tre livelli, solo un sottoinsieme di funzionalità del contratto intelligente viene implementato sulla blockchain Ethereum. La complessa logica di business è rimossa

dal percorso di esecuzione, il che permette ai livelli di dati di essere ottimizzati per riflettere la natura distribuita della rete.

Le componenti del pacchetto di contratto intelligente implementato sulla blockchain Ethereum sono lo schema database, la validazione e verifica delle transazioni che sono aggiunte al ledger (registro generale), e la logica di ottimizzazione richieste per leggere il ledger. La logica di business è portata al di sopra della blockchain Ethereum, su uno strato mediano (business) separato. Tale codice logico accede ad una varietà di servizi, inclusi l'esecuzione sicura, l'attestazione, l'identità, il supporto crittografico, formattazione dati, il messagging affidabile, trigger, e l'abilità di legare quel codice allo schema in contratti intelligenti specifici su qualunque numero di blockchain, permettendo a Patientory di venire usato all'interno di vari consorzi d'assitenza sanitaria in modo facile e diretto. Questi servizi sono forniti in una struttura in cui i singoli pezzi di codice che sostengono i contratti intelligenti vengono eseguiti, mandano transazioni ai nodi blockchain, e sono vincolati allo schema a livello dei dati.

Vantaggi Unici Aggiuntivi

Sebbene un'istituzione medica come un ospedale non dovrebbe avere accesso a registri che non sono stati specificatamente approvati, l'utente finale potrebbe derivare beneficio aggiuntivo dalla partecipazione al servizio per via della pre-autorizzazione per gli utenti di condividere le informazioni in circostanze di emergenza. Tenendo questo bene a mente, il necessario accesso da parte delle strutture mediche ai registri di una persona priva di conoscenza rende sensato l'estensione dei privilegi d'accesso se l'utente lo ha precedentemente autorizzato. Nel caso in cui una persona è priva di conoscenza, e porta con sè il cellulare, l'istituzione può provare la proprietà del dispositivo dell'individuo utilizzando un metodo di firma secondario che è disponibile dalla schermata di blocco di uno smartphone. La seconda chiave non deve essere la stessa chiave privata dell'accunt primario. Così, se l'account di un'istituzione ha inviato una firma d'emergenza, la blockchain può estendere i privilegi d'accesso per permettere l'accesso prima bloccato ai registri medici. **Questa chiave privata dovrebbe essere considerata bruciabile ed essere rimpiazzata dall'individuo il prima possibile. In questo modo, lo scambio sicuro di informazioni tra un individuo e un'istituzione autorizzata può essere facilitato in condizioni d'emergenza.** Dovesse un'istituzione richiedere queste informazioni senza l'appropriata autorizzazione, l'individuo verrà notificato della cosa. Se l'individuo rifiuta questa richiesta all'interno di un'intervallo di tempo limitato, i dati non sono condivisi. Inoltre, se un'istituzione dovesse effettuare molteplici tentativi di richiesta fraudolenti, l'istituzione può essere punita con la revoca dei privilegi, pene monetarie, e/o azioni legali. Il danno

causato dalla perdita del cellulare è minimo poiché vi è bisogno sia del dispositivo che di una chiave di livello istituzione. Nel futuro prossimo, tutte le carte d'assicurazione potrebbero includere micro-controller crittografici come quelli presenti nelle moderne carte di credito, che faciliterebbero la stessa operazione in assenza dello smartphone.

Priorità d'Assistenza Sanitaria Nazionale/Internazionale

Cure PersonalizzatePersonalized Care

Per ottenere efficaciemente cure migliori è necessario un approccio incentrato sulla persona. Un tale approccio deve tenere conto degli aspetti clinici nonché dei fattori sociali ed economici che ostacolano l'abilità di qualcuno a rispettare le modalità d'assistenza e di vita salutare necessarie al mantenimento di un benessere sostenuto.

Ottenere esiti delle cure efficaci richiede l'identificazione chiara delle situazioni di vita e delle barriere alla salute individuale. Con il crescente numero di pazienti con 2 o più morbi, l'approccio all'assistenza sanitaria “chiusa in silos” e “uguale per tutti” non conduce all'incitazione e l'affronto di esiti delle cure efficaci. Perciò deve essere esaminato un modello di assistenza più flessibile disegnato per includere i bisogni variegati di salute e benessere dei pazienti. Ciò richiede che sia di vitale importanza un piano d'assistenza completo, dinamico e interattivo in cui il paziente possa attivamente tracciare, gestire e partecipare nelle proprie cure individuali.

Esiti Clinici

Misure per gli esiti relativi ai Pazienti (PROMs), che si concentrano sugli esiti che sono direttamente collegati al paziente, hanno assunto maggiore importanza e rilevanza negli ultimi anni. Ciò è dovuto, in parte, alla maggiore attenzione prestata all'esperienza dell'assitenza da parte del paziente e all'analisi sul carico e l'impatto della malattia incentrato sul paziente. I PROM possono includere sintomi e altri aspetti degli indicatori sulla qualità della vita legati alla salute quali funzione fisica o sociale, fedeltà al trattamento, e soddisfazione per il trattamento. Possono anche facilitare una comunicazione più accurata paziente-dottore in termini di peso dei morbi legati al trattamento fornendo una stima più dettagliata e completa dei trattamenti per condizioni specifiche quali il cancro o la sclerosi multipla.

I PROM si distinguono dalle misure dell'efficacia clinica tradizionali (es. Sopravvivenza al cancro, smettere di fumare) perché riflettono direttamente dalla prospettiva del paziente l'impatto della malattia e il suo trattamento. Tali misure possono esaminare l'equilibro tra l'efficienza del trattamento e il suo gravare sul paziente. È anche efficacie nell'osservare aree quali il funzionamento fisico e il

benessere complessivo, nonché sottolineare l'efficacia e la sicurezza dei trattamenti in relazione ai benefici clinici complessivi. Poiché le misure stesse sono sviluppate dalla prospettiva del paziente, può facilitare il maggiore coinvolgimento del paziente nelle decisioni che riguardano il trattamento e fornire una guida per le decisioni legate all'assistenza sanitaria. Essenzialmente, rafforzare una struttura di blockchain PROM rafforza l'abilità di incentivare I medici curanti e I paganti a rispettare gli standard delle cure.

Conclusione

La blockchain giocherà un ruolo sempre più importante nell'IT dell'assistenza sanitaria e porterà dei vantaggiosi cambiamenti e nuove efficienze ad ogni stakeholder nell'ecosistema. È di vitale importanza che le organizzazioni sanitarie comprendano il fulcro della tecnologia blockchain per assicurarsi di essere pronte ai cambiamenti che la tecnologia porta con sè.

Il risultato sarà una nuova generazione di potenti applicazioni basate sulla blockchain che daranno forma alla prossima era del business nell'assistenza sanitaria. Perché la blockchain esprima il suo potenziale nel settore dell'assistenza sanitaria, deve essere basata su standard che assicurino la compatibilità e l'interoperabilità all'interno del scenario del sistema “chiuso in silos” dell'assistenza sanitaria attuale.

Riferimenti

[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 ap- plication platform. White Paper". In: (2014.).

[6]Yan-Cheng Chang and Michael Mitzenmacher. "Privacy preserving key- word 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 Bal- ance 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: Digitis- ing 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 Pri- vacy 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 sys- tems: from system, syntax, structure to semantics. In Interoperating Ge- ographic 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..