

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

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

May 2017

Ang dokumentong ito ay pagbibigay impormasyon lamang at hindi nangangahulugan ng pag aalok o pagbebenta ng shares o securities sa Patientory o kahit anong kaugnay na kumpanya. Ang ano mang pagbebenta ng shares o securities ay mangyayari lamang sa pamamagitan ng konpidensyal na liham o kasulatan sang ayon sa lahat ng umiiral na batas at alituntunin patungkol dito.

Abstrak

Ang blockchain powered health information exchange (HIE) na ito ay kayang malaman ang totoong kahalagahan ng interoperability at cyber security. Ang sistemang ito ay maaaring makaalis ng gastos sa kasalukuyang third party intermediaries, kung ating titignan ang pangangasiwa sa maayos na populasyon. Makasisigurong may magandang data integrity, pagbawas sa gastos sa transaksyon, at pagkakaroon ng tiwala sa isa't isa. Kakayanan upang makaugnay sa patient care sa pamamagitan ng blockchain HIE ay makakatulong upang mabawasan ang di inaasahan services at pagkakaulit ng tests at sa mababang halaga at maayos na continuum care cycle, habang sumusunod sa lahat ng probisyon ng HIPAA. Ito ay proseso na nakasentro sa pasyente na suportado ng blockchain technology, binabago na ng Patientory ang pamamaraan ng pangangasiwa ng healthcare stakeholders ng electronic medical data at kung papaano sila makikipag usap sa mga clinical care teams.

1 Panimula

1.1 Ano ang Blockchain?

Ito ang teknolohiya sa likod ng bitcoin digital currency, Ang blockchain ay nalikha ng hindi pa nakikilalang tao (o grupo) sa likod ng pangalang Satoshi Nakamoto. Simula 2009 ang blockchain ay mas nakilala sa larangan ng finance industry, at ng iba't ibang blockchain-enabled businesses at iba pang serbisyo na pumapasok sa market. Ang teknolohiya ng Blockchain ay ginagamit sa paglalathala ng ledger ng transaksyon para sa maraming business network na walang iisang indibiduwal na mukukontrol. Ang Ang ledger na nakikita ng lahat ay lumilikha ng mas madaling

pagkita sa commercial relationships kung saan makikita at malalaman ng lahat ang nangyayari at mamari silang makipagtransaksyon ng hindi kinakailangan ang central point of control. Ang Teknolohiya ay naglalagay ng privacy at control ng data sa bawat indibidwal at ang tiwala at integridad ay nabuo ng hindi kailangan ng third-party reliance intermediaries.

1.2 Kasalukuyang Healthcare Infrastructure

Ang pagbabago mula “procedure” based focus papuntang “holistic care of the individual” ay nangangailangan na ang Care Providers ay bumuo ng “samahan” na magsasama-sama gumawa upang makamit ang isang layuning paunlarin ang kalagayan ng kalusugan ng pasyenteng inaalagaan, para sa post-acute care episodes o sa pagitan ng acute care episodes. Ang pangangailangan sa pagkakaisa sa pagitan ng care-providers mula specialists, primary care physicians, caregivers at wellness providers (tulad ng nutritionist and rehabilitation nurses) ay nag reresulta ng pagtaas ng paggamit ng digital technologies. Kahit na ang mga solusyon na ito ay may malaking pagbabago sa paghahanap at maayos na pagbibigay serbisyo, ang mga ito ay nagresulta sa paglikha ng maraming impormasyon patungkol sa kalusugan, lalo na sa electronic medical records (EMR) systems.

Ang organisasyon pang kalusugan at ang gobyerno ay gumagastos ng malaking salapi at oras upang mabuo at maayos ang traditional na impormasyong pang kalusugan at pagpapalitan ng data; nangangailangan ng salapi upang patuloy na malaman ang mga issues, update field parameters, perform backup at recovery measures, at kumuha ng impormasyon para sa pagpapaliwanag.

Ang Federal laws at incentive programs ay ginawang mas accessible ang health care, bilang tugon sa pagpigil ng mga ospital sa pagpapatupad ng EMR. Subalit, ang nakakaraming mga ospital ay hindi pa rin kayang maibahagi ng mabilis at ligtas ang kanilang datus. Bilang resulta, ang mga doctor ay naglalaan ng mas maraming oras habang nata-type kaysa sa pakikipag usap sa pasyente. Tumaas din mula 45 papuntang 54 porsyento sa pagitan ng 2011 at 2014 ang pagkapagod ng mga doctor [1].

Kahit na may sinasabing “individualized” health information sa parehong clinical at wellness front, ito pa rin ay hindi nagangahulugan ng “personalized” na plano ng pangangalag. Gayunpaman, kahit marami nang datus ang pangkalahatang healthcare ecosystem ay hindi pa rin sila makabuo ng paraan upang mas mapalaki ang kanilang datus upang mas malaman nila ang marami pang uri ng pangangalaga sa pasyente.

Kung kaya’t ang kasalukuyan solusyon na ginagawa ng mga Health Care technology industry ay nagresulta sa pagpili sa pagitan ng privacy/economic fraud para sa pasyente. Nakikita natin ang problemang ito habang lumalaki ang datus na nalilikha ng industriyang ito. **Ang na seguridad ng blockchain**

technology, properties, at distributed nature ay makakatulong mapababa ang gastos at maayos na paggamit ng ligtas na infrastructure.

1.3 Ang Relasyon ng Pasyente sa Provider

Ang bagong healthcare paradigm ay nangangailangan ng epektibong at demands the need for effective and magandang pagbibigay ng serbisyong pangkalusugan para sa mas maraming magagandang resulta nito. It ay nangangailangan na ang Principal Care providers ay may kakayahang makipag usap at makapagpalitan ng pananaw sa iba pang ancillary health organizations na kasama nila gaya ng mga laboratory at botika. At upang maisakatuparan ito, kailangan nila ng updated at modified na impormasyon ng pasyentelagi araw-araw.

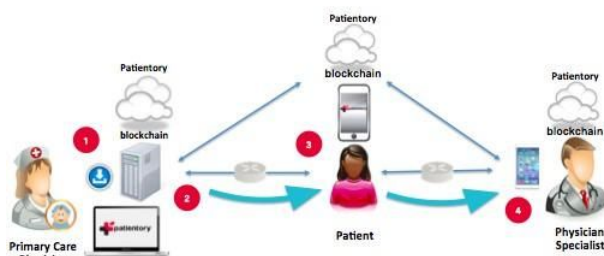


Figure 1: Patientory Schematic

Ang EMR software ay kasalukuyang pinipigilan ang epektibong ugnayan ng pasyente ng ng kanilang mga provider at ang Patient portals ay may malimit na paguusap sa mga pasyente na nagreresulta sa pagiging mag isa ng pasyente. Dagdag pa dito ang software na ito ay nagbibigay lamang ng limitadong kakayahan sa pagpapalitan ng impormasyon mula sa isang sistema pamunta sa iba na nangangailangan ng isang bihasang indibidwal sa paglilipat ng impormasyon. Ito ay nagresulta sa maraming paghinto sa pagbibigay ng lunas ng mga organisasyon at nag resulta ng pagbaba ng kaayusan ng pangangalaga sa kalusugan ng mga pasyente. Habang gumugul ang mga care providers ng maraming oras sa pag uugnay ng mga benepisyo, ang kanila ding epektibo sa pagbibigay lunas sa pasyente at dami ng trabaho ay tumaas din. Ito ay nagresulta ng kabaligtarang epekto sa pagbibigay kalinga sa mga pasyente.

Karagdagan pa dito, marami sa mga doctor ang ayaw pahintulutan ang pasyente sa kanilang EHR, kung kaya't gumagawa ng kakaibang paraang ang mga pasyente upang malaman ang lagay ng kanilang kalusugan. Ito ay nagbibigay ng hindi magandang epekto sa mga pasyente dahail sa tingin nila ay wala silang control sa lagay ng kanilang kalusugan at nagreresulta sa hindi nila pagpasin sa kanilang kalagayan. Kahit na may malaking pagbabago dahil sa mga Mobile Health Care apps na tumutulong sa mga indibidwal upang malaman ang kanilang

kalagayan, ngunit ang hindi pa rin sila sapat upang magkaroon sila ng tamang kaalaman na mailalahad lamang sa EHR.

2 Sulyap sa Sistema

Ang problemang ito ay sinusuluyon ng paggamit ng Patientory Blockchain Network. Ang Legacy EMR ay sentralisado at maaaring pasukin ng mga hacker, may mataas na seguridad, at may malaking gastos. Sa pagpapatupad ng Patientory Blockchain infrastructure, ang mga providers ay makakaiwas sa mga possible kakulangan dahil sa inherent access control properties ng sistemang ito; isang daan sa pag-uugnay ng mga benepisyo na nagresulta sa pag-papaunlad sa kalusugan. Ang nasa itaas ay schematic na nagpapaliwanag ng Patientory blockchain infrastructure at ugnaya sa pagitan ng mga pasyente ng kanilang mga providers.

3 Pagpapatupad ng Sistema

3.1 Ang Regulasyon at Alituntunin ng HIPAA

Bago ang makahulugang kaalaman patungkol sa pagpapatupad ng sistemang ito, ang mga batas at alituntunin ng mga probisyon ng Health Insurance Portability and Accountability Act of 1996 (HIPAA) ay kailangan munang mabigyang pansin. Ang kauna unahang bagay na kailangan ng pansin ay ang Privacy Rule, Security Rule, at ang Cloud Computing Guidelines. Ang layunin ng dokumentong ito ay hindi upang malaman ang kabuuan ng HIPAA law. Ang mga mahahalagang detalye lamang sa sistemang ito ang bibigyan pansin sa tamang pagkakataon.

A. Privacy Rule

Ang business model ng Patientory ay nagpapahayag na ang Privacy Rule requirements ay kailangan masunod dahil sa electronic storage at paghahatid ng pribadong impormasyon sa kalusugan. Ang pagpapatupad ng privacy rule ay nilahad ng ganito, “Ang Privacy Rule... (na ginagamit) sa health plans, health care clearinghouses, at sa anumang healthcare provider na naghahatid ng impormasyon gamit ang electronic form” [2]. Karagdag pa dito, ang iba pang partidong na kumakatawan sa kanila bilang service providers, ay responsible din na sumunod sa HIPAA. Ang mga ahenteng ito ay tatawaging Business Associates (BA), at ang mga legal na alituntunin na kailangan sundin ng BA ay nakalagay sa tinatawag na Business Associate Contract (BAC) at ang HIPAA ay nagbibigay ng istriktong pansin sa pagsunod sa mga napagkasunduan dito.

Ang pagbibigay pahintulot ay nakasaad pagbibigay pahintulot sa paggamit ng impormasyon, ang gamit ng de-identified information, at ng kahulugan ng private information. Ang Private health information (PHI or ePHI for electronic data) ay binigyang kahulugan bilang “lahat ng maaaring malamang impormasyon sa kalusugan na hinahatid ng kahit anong ahente sa pamamagitan ng kahit anong paraan, sa electronic, papel, o sa salita man” [2]. De-Identified health

information ay binigyan kahulugan bilang “Health information na hindi tumutukoy sa isang indibidwal at walang tamang basihan upang paniwalaan na ang impormasyon ay naglalarawan kahit kanino man at ito ay hindi kayang tumukoy sa iisang health information” [2]. Ang de-Identified data use restrictions ay nangangahulugang, “Walang pagbabawal sa paggamit ng de-identified health information. De-identified health information na walang basehan upang kumilala sa sino mang indibidwal” [3]. Ang pagitan ng identifiable data sa de-identifiable data ay ang anumang impormasyon na maaaring pagbawalan ang indibidwal sa at mga loleksyon ng mga impormasyon na may kinalaman sa hindi bababa sa 0.04% ng kabuuang papulasyon sa US.

B. Security Rule at Cloud Computing Guidelines

Dahil sa haba ng mga nilalaman na kasama sa araling ito minainam naming ilahad na lamang ang mga bagay na sadyang makatutulong. Ito ang mga mahahalagang detalye, “Kapag ang anumang bagay ay nasama sa serbisyo ng CSP upang lumikha, tumanggap, magpanatili, o magpadala ng ePHI (such as to process and/or store ePHI), sa pamamagitan nito, ang CSP ay isa nang business associate ayon sa HIPAA. Gayun din, kung ang business associate subcontracts na may CSP na lumikhato, tumanggap, magpanatili, o magpadala ng ePHI pamalit dito, ang CSP subcontractor ay isa na ring business associate. Pareho pa rin ito kung ang CSP ay nagpoproseso o nagtataglay lamang ng encrypted ePHI at walang encryption key para sa datus. Ang kawalan ng encryption key ay hindi nagbibigay daan upang hindi maisama ang CSP sa business associate status at mga pananagutan ayon sa alituntunin ng HIPAA. Bilang resulta, ang covered entity (or business associate) at CSP ay kailanagn sumunod sa HIPAA-compliant business associate agreement (BAA), at ang CSP ay parehong responsable sa pagsunod sa mga kasunduan ng BAA at direktang kailangang sumunod sa lahat ng alituntunin ng HIPAA Rules” [3].

Ang covered entities ay kadalasang gumagamit ng cloud storage providers (CSPs) upang paglagyan ng impormasyong pangkalusugan, at ito ay madalas na sinasabing mas mabisa at may mababang IT management costs. Ngunit dahil ang mga consumers ang umaasa sa cloud providers upang paglagyan ng personal data, ay nawawalan sila ng direktang kontrol sa kanilang datus at bilang resulta walng may alam kung sino ang may access at kung saan talag nakalagay ang kanilang mga datus. Kahit na ang explicit business associate agreement ay binuo sa pagitan ng BA at ng cloud storage provider, ito ay nagpapahayag lamang ng mga alituntunin na kung sino ang responsible sa privacy at security ng data kung mayroong hindi susunod. Ang mga consumer ay maaaring magkaroon ng control sa data streams, ngunit hindi pwedeng umasa sa cloud storage provider upang ipatupad ang mga pribelehiyo nito.

Kahit na kilala ang paggamit ng cloud storage, mayroon pa rin itong mataas na pagkakataon na panganib na ang consumer ay kumontrol gamit ang mekanismo ng kanilang personal data. Sa cloud-based architecture, ang data ay madalas nagagayaat at naaalís, kung kaya’t ang panganib ng paggamit ng unauthorized data ay tumataas. At marami ring indibidwal ang napagbibigyan na

maka-access sa mga datos, gaya ng administrators, network engineers, at technical experts na gumagawa para dito, o para sa servers that host this data. Tumataas din ang panganib ng unauthorized access at use dito.

Ngunit kahit na ang data ay ligtas gamit ang strict access controls at encrypted sa point of origin at habang nasa transit, ito ay nagtataglay pa rin ng problema para sa pag unlad ng Patient-Reported Outcomes Measures (PROMs). Ang konsepto ng PROM ay upang paunlarinang patient-focused measure na may kinalaman sa isang area o focus na may kinalaman sa pasyente, na kung saan ang kanilang makikipag usap at makikipag ugnayan ay mahalaga upang ito ay mapatupad. Ang pag-access ng malaking data streams mula sa iba't ibang gamit ay parte ng IoT network, na ginagamit ngayon sa cloud based services ay maaring magpa unlad ng pundasyon ng PROM, ngunit mahirap malaman kung ang datos na ito ay nasa cloud at lilikha ng ng pamamaraan na makabuluhan para sa pasyente.

Ang paggamit ng blockchain technology para masiguro at mapaganda ang data security ng medical records na kaugnay ng sistemam ay maaaring magpawala ng health breaches at magpa-decentralization ng record ownership. Ang proseso ng encrypting data kapag pinapadala sa database gamit ang iba't ibang algorithms at pag-decrypt nito habang nagrere-trieve ang gagamitin. Ang data ay isulat gamit ang NIST compliant algorithms sa tuwing nagpapadala at kumukuha ng detalye al dahil ito'y itinakda ng batas. Kaya ang palitan ng impormasyon ay dapat sumunod sa lahat ng alituntuning itinakda sa NIST specifications.

Dahil sa maraming bilang ng data breaches na kinakaharap ng healthcare industry, ang blockchain technology ay ginawang HIPAA compliance feasible ang parehong pasyente at mga providers.

C. Blockchain System Analysis of Limitations due to HIPAA Restrictions

Ang Ethereum Blockchain ang nagaayos ng diverse subset ng system implementations dahil sa application ng Turing complete programming language na ginagawa ng Ethereum Virtual Machine. Ang sistemang ito ay may limitasyon sa at walang direktang panlabas na inspeksyon sa masmalawak na internet maliban sa paggamit ng Oracle Services. Karagdagan pa dito ang limitasyon ng storage ng blockchain ay inapamahalaan ng gas cost of storage at gas cost of access sa datos na ito. Sa pagsulat na ito, ang block time ng chain ay gumagawa ng minimum bound para sa state modifying requests sa loob ng 15 segundo.

Ang limitasyon ng blockchain para maglaman ng pribadong ipormasyon ay maaring malabanan sa pamamagitan ng data obfuscation, gaya ng encryption, ngunit kung ang decryption key ay kumalat ay wala nang paraan upang matanggal ang mga sensitibong datos mula sa blockchain. Para sa HIPAA compliant data, ito ay maaaring magresulta sa paulit ulit at di na maaayos pang pagkalat ng impormasyon dahil sa immutability ng blockchain it. Kahit na ang de-identified data ay maaaring paglagyan ng Public Ethereum Blockchain, ito ay magiging masalimuot kung ating iisipin na ang de-identification na nagsasala sa

mekanismo ay hindi papalpak, o ang sideband information na kasama sa blockchain interactions ay hindi kayang ilabas ang totoo nitong pagkakakilanlan. Ang konklusyon ng ito ay nagging konklusyon na rin ng MIT Media Lab sa panahon pagbuo nila ng MedRec Protocols at binood sa MedRec Whitepaper [3]. Ang pagmimina ng sideband information ay maaring kasing simple ng pagtingin sa timestamps at interakosy sa kilalang data storage contracts.

Sa pananaw na ito ay posibleng maipalagay na ang indibidwal sa institusyon, at ang mas mahalaga ay ang oras na kung saan sila naroroon sa facility. Sa pagbibigay ng specialized nature ng ibang facilities, ito ay sapat na impormasyon upang magkasala sa HIPAA compliance dahil sa kakayanan ng makakakita na magpahayag ng parehong pagkakakilanlan, lokasyo, oras ng interaksyon, at maaaring uri ng diagnosis.

Dahil ang lokasyong ito ay nagiisa at walang kasama, ang pagbawas sa 0.04% ng populasyon ng US ay wala nang halaga. Ang katotohanang ito ay bumubuo ng di makatwirang punto na pagkakamali na dapat nating malaman. Karagdagan pa dito, ang direktang lagayan ng even encrypted information sa blockchain ay lumilikha ng pananagutan sa database managers na pumasok sa BAC dahil sa kanilang aksyon bilang HIPAA data storage facility (See section titled Security Rule and Cloud Computing Guidelines). Ito ay isang hindi makatwirang ekspektasyon dahil ang bawat miner at ang bawat indibidwal ay nagdadala ng passive nodes, at kailangan maging HIPAA compliant. Dahil dito name ay nagpatupad ng mekanismo para sa patuloy na storage of sensitive information sa pamamagitan ng private implementation ng Ethereum based blockchain.

D. Ang pagpapatupad ng mga layunin para sa maayos na paggamit at seguridad

Ang pangunahing layunin ng kahit anong secure system ay maaaring mabuod bilang sa mga layuning ito: confidentiality, integrity, availability, accountability at information/identity assurance. Upang malamam ang mga layunin, ang attacker at user ay kailangang maintindihan. Ang bawat gampaning ito ay nangangailangan ng ng pagkilala sa kanilang abilidad. Mula sa pananaw ng user, ang system ay kailangang maging sufficiently transparent upang hindi na mangailangan pa ng anumang advanced knowledge. At dahil mahirap na maindindihan ng mga normal user sa ang komplikadong cybersecurity, ang proseso ay dapat hindi basta bastang maapektuhan ng ginagawa ng mga user.

Kung sakaling may umatake sa sistema, ito ay lilikha ng ng bilang ng bagay na kailangang ilagay sa compromise resource na mas malaki ang halaga kaysa sa totoong halaga nito. Ito ay dahil sa katotohanang ang mga sufficiently advanced party na may maraming resources ay may kakayahang hindi sumunod sa anumang sistema sa loob ng tamang oras at kakayahan. Wala naming kasing perpektong depensa. Sa mga limitasyong ito sa ating pagiisip, ang pagpapatupad nito ay patuloy nating pag-aaralan sa kung papaano natin nakamimit ang mga layuning unang nabanggit.

3.2 Ang Kahulugan ng Hardware at Network Implementation

Upang maisama ang mga disenyo ng mga layuning nabanggit, ang mga selected system implementation ay mangangailangan ng ibang independent systems. Ang bawat system ay hinahati ang authority upang masiguro na ang mga authorized entities lamang ang makapag ugnay ng tama at para gumawa ng ligtas na mekanismo upang mapataas ang seguridad habang pinapanaili ito. Ang sistemang ito ay ginawa rin upang ang scaling ay maaring matapos sa pamamagitan ng pagdagdag ng hierarchical calling schemes. Ang sistemang ito ay idinetalye sa baba.

Ang public facing entity ay isang Remote Procedure Call (RPC) Server na namamagitan sa private implementation ng Ethereum Blockchain (permissioned blockchain). Ang grupong ito ng blockchain nodes, ay maaari lamang maisama sa ibang blockchain nodes, sa key authoring entity, sa HIPAA compliant storage facility, at sa RPC Server. Ang key authoring entity ay isang resource na gumagawa ng private/public key pairs para sa blockchain. Ang HIPAA compliant storage facility ang nagdadala ng tamang data na bumubuo ng electronic private health information (ePHI).

Kapag may humihingi ng data, pwedeng pahintulutan ang HIPAA compliant system na kumausap sa forwarding agent, na sya naming magdadala ng data papuntang RPC server. Maaari rin naming baguhin ito na maging direktang makipag ugnayan ang HIPAA storage sa RPC server. Ang bawat pagpapatupad ay may benepisyo na kailangang isipin bago ang huling pagpili. Sa kahit anong pangyayari, ang HIPAA storage facility ay dine-decrypts ang mahalagang bahagi ng database. Itong decrypted information ay irere-encrypted gamit ang public key ng requesting party para maipadala. Ang public key na ito ay public key rin ng contract na tumatayo bilang control interface mula sa blockchain papuntang HIPAA data.

Ang diagram ng specified network topology ay makikita sa figure 2.

3.3 Ang Kahulugan ng Software Implementation

Karagdagan sa physical isolation ng systems sa hardware at network implementation, ang software ang kumukontrol sa integridad ng data at Topography verification ng authorization para sa humihiling nito. Ang software system, mula sa pananaw ng access control at data encryption ay nasa ibaba.

Ang HIPAA compliant database ay tatanggapin lamang ang inbound connections mula sa HIPAA forwarder. Pinapanatili nito na ang daloy ng traffic ay para lamang sa kilalang controlled paths. Ang HIPAA forwarder ay kikilos lamang na mag forward ng request sa HIPAA storage facility kung may pending valid transaction ang nangyari sa blockchain, at ang transaksyong ito ay nagreresulta sa emission ng requesting event. Ang requesting event ay nangangailangan ng public key ng requesting party at ang mga data fields na hinihiling. Sa huli ang RPC server ay gumagamit ng access controlled Application

program interface (API) na ang kilalang users lamang ang pwedeng makisama sa server.

Upang maintindihan ang call hierarchy ng system, ang contract structure to facilitate access control ang kailangang unahin. Ang bawat user ng system maps sa private address ng private blockchain. Ang bawat private address ang pwede lamang makipag ugnayan sa IISANG contract sa block chain.

Figure 2: Patientory Blockchain Network

Ang contract ay ang class contract ng bawat indibidwal. Ang institutions, institution employees, at customers ang class level objects.

Ang mga class level objects ay permission-based interfaces. Ang Institution Contract ay mayroong listahan ng lahat ng customers na may kakayahang makakita sa mga institution at ang bawat customer contract ay may listahan din ng institutions na binigyan ng permiso. Ang contract na nasa institution ay may tungkulin na pangunahan ang anumang paghinto sa pagpapahintulot sa institution, mula sa user. **Ang institution contract ay hindi maaring mabago ang listahang ito, kaya mapipigilan ang hindi awtorisado na makakita sa record ng indibidwal.** Karagdagan pa, ang Institution Contract ay nagtataglay ng listahan ng authorized employees na kayang magpanatili nito. Ang permission scheme ay dapat gumawa ng automatic revocation of a permission sa semi-regular intervals para maiwasan ang institution mula sa di inaasahang pagpapanatili sa karapatan ng nakaraang mga empleyado.

Sa sistemang ito, lahat ng external parties ay mag-uugnayan sa pamamagitan ng pagbibigay ng signed transactions na maglalagay ng requesting call. Ang transactions ay ipapasa sa pamamagitan ng RPC server pagkatapos masuri. Ang RPC server ay maglalagay ng requests sa data aggregation server na sya naming magpapadala ng mga requests na ito sa mga miners base sa load sharing mechanism. Ang miners ngayon ay maaari nang magproseso ng request gamit ang pagpapasa ng transaction kapalit ng calling party patungo sa party's respective controlling contract. Ang kontratang ito ay may permiso ng data na ang sinuman ay authorized para i-access ng internal sa contract. Ang kontratang ito ang nagiisang entity na tatanggap ng transaction mula sa labas. Kaya ang mekanismong ito ay ginawa upang makontrol ng buo ang call operations sa blockchain.

Ang bawat transaksyon, ang hindi mababagong record ng calling party ay nalilikha. Pinapanatili nito na ang bawat pagbubukas sa impormasyon na mangyayari ay malilista. Ang totoong data na nakalagay sa user contract ay system ng hash pointers na kapag naayos ng HIPAA storage server ay magreresukta sa pagbabalik ng tamang data. Ang impormasyong ito ay ipapadala sa HIPAA forwarder sa pagpapatupad ng valid request transaction. Ang mekanismong naguugnay dito ay hindi direkta at nagihahayag gamit ang blockchain event messaging system. Dahil sa limitasyon na ang requester ay maaari lamang magtanong patungkol sa database gamit ang valid transaction, at ang user ay hindi maaaring direktang baguhin ang kanyang impormasyon ang access control ay talagang napatunayan. Mula sa pananaw ng institutions, ang mekanismo ay pareho maliban sa institution contract ay naglalaman ng listahan ng users mula sa kung saan ito maaring humingi ng data at listahan ng users na maaaring makpagugnayan sa institution bilang magagawa. Kapag ang request transaction ay nagmula sa contract ng institution employee, ang kumokontrol ng contract at tatawag sa institution contract, na sya naming tatawag sa user contract upang hingiin ang data pointers na reresulba sa ePHI. Pending the institution ay nasa listahan ng approved institutions para sa user, at ibabalik ng

contract ang tamang hash pointers. Ang pointers ay ipapakita din bilang event message na ipapadala muli sa HIPAA storage facility.

Sa paglilinaw, ang buong proseso ng single request ay ganito: Ang external party ay magre-requests ng data mula sa service gamit ang pagtawag sa RPC server na may cryptographically signed transaction para ipasa sa blockchain. Ang RPC server ay tutukuyin ang external party's identity gamit ang signature ng login request.

Ang pagpe-pending ng signature na magtutugma sa entry sa database ng pinayagang public keys, ang RPC server ang tatanggap ng request at magpapasa ng request sa Data Aggregate Machine. Ang Data Aggregate Machine naman ang magpapasa ng requests sa pribadong blockchain verifiers. Ang verifiers ay makakatanggap ng request bilang tawag sa blockchain account laban sa target contract. Ang verifiers ang gagawa ng tawag, at kung ang request ay papayagan ang transaction ay isusulat sa next block. Ang transaksyong ito rin ay nagdudulot ng palabas ng event message sa blockchain. Ang event message ay tinitignan ng HIPAA Forwarder, na tumatayo upang gumawa ng encrypted request laban sa HIPAA storage based sa pagkalitong dulot ng event message. Ito rin ay naglalaman ng public key ng requesting party. Ang HIPAA compliant database system ay tinitignan ang request at nagpapadala ng encrypted copy ng impormasyon sa RPC server gamit ang public key ng requesting party. Ang RPC server ngayon ang magbabalik ng impormasyon sa requesting party gamit ang remapping ng requesting IP sa public key sa message. Ang RPC server naman ang magpapadala ng message na kahit hindi nakikita ang underlying data. Ang data na ito ay sisrain agad ng RPC server, at sisiguruhing ang RPC server ay gagawa bilang daan na hindi kailanganng maging HIPAA compliant.

Ang mekanismo upang ilabas ang data ay parehong muli ngunit ang data na ipapadala ay encrypted na may public key ng HIPAA storage facility. Ang ibang operations ay kapareho maliban sa data na nilagay sa bubbles up gamit ang event message system. Kaya dahil sa gamit ng low collision hashing functions at timestamped nonces, ang data ay maaari nang mailagay kasama ang contract na kayang mag compute ng address sa kung saan nakalagay ang pinadalang data sa HIPAA storage facility.

Sa huli, ang pamamahagi ng private keys sa entities ang kailangang solusyunan. Ito ay maaring pangunahan gamit ang optical means sa mga smartphone users. Ito ay pareho sa gamit ng QR codes bilang address para sa Ethereum addresses. Ang ibang paraan ay maaari ring magawa gamit ang applications sa parehong desktop computers at tablet/smartphone devices. Ang pagkawala ng key ay hindi masamang bagay, dahil sa kakayanang maalis ito at mailipat ang access control sa iba.

3.4 Interoperability

Ang EHR systems ay base sa isolated credential validation architecture na kung saan ang datus ng pasyente ay nakatago sa magkakaibang systems. Ito ay

nagresulta sa one-toone care co-ordination software “add-ons” na nagging solusyon sa sistemang ito na makipagugnayan para sa coordination of care sa iba pang providers at ancillary health organizations. Ngunit, ang pagkuha ng impormasyon mula sa principal Provider organization papunta sa ibang organizations ay limitado lamang sa pamamagitan ng to Read, to Submit, to Send or to Notify. Kaugnay pa nito ang Patient/Consumer ay may limitadong interakyon lamang o pagpapalitan ng impormasyon. Dagdag pa dito ang hindi maganda sa existent mechanisms ng data exchange ay ang mahirap na pgsasaayos ng mga mali na nagyari habang pinapasa.

Kapag ang blockchain at ang smart contracts ay naayos, ang parameters ay magiging absolute. Ang pasyente ang magiging primary intermediary sa pagpapadala at pagtanggap ng impormasyon sa kanilang kalusugan at pawawalang bisain ang pangangailangan sa madalas na updates at troubleshooting sa anumang software. Dahil ang blockchain records ay hindi nababago at nakalagaysa lahat ng participating users, ang recovery contingencies ay hindi na kailangan. Maliban pa dito, ang blockchain’s transparent information structure ay maaaring alisin ang maraming data exchange integration points at ang takaw oras na reporting activities.

3.5 Processes and Scalability

Ang users ang may control ng lahat ng kanilang impormasyon at at naglilipat nito at dahil dito napapanatili ang mataas na kalidada ng data na complete, consistent, timely, accurate, at widely available kaya ito ay magiging kagamit gamit at mapagkakatiwalaan. Dahil sa decentralized database ang blockchain ay wala nang sentro ng pagkakamali at mas maganda nang labanan ang mga malicious attacks.

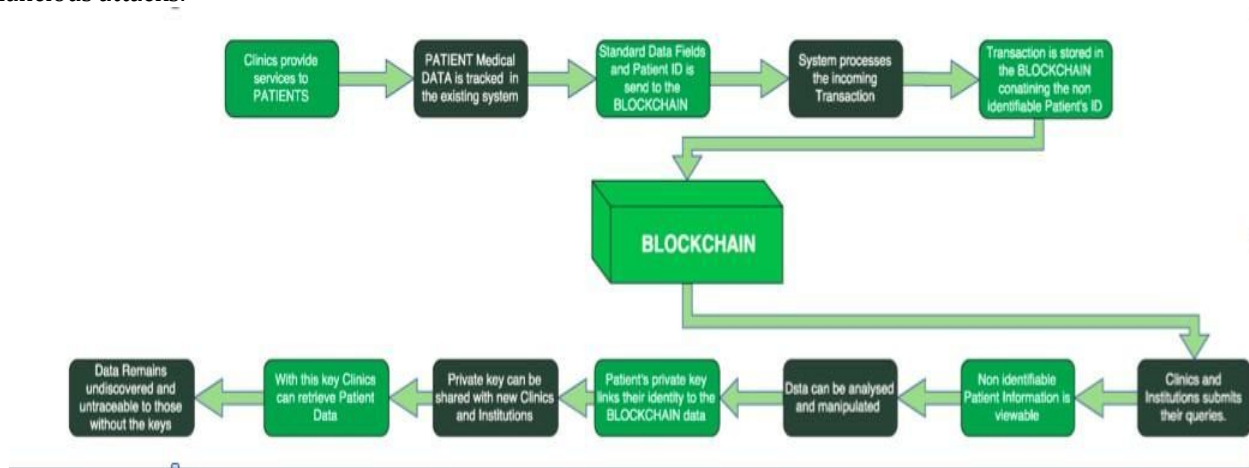


Figure 3: Blockchain Process Flow Diagram

Sa anumang Care network mahalagang panatilihin na ang lumalahok ay nakikipagtulungan sa bawat isa at maaaring magtiwala sa isa't isa sapagbibigay ng nararapat na serbisyo na kailangan nilang gawin. Upang mangyari ito, kailangan nating magkaroon ng accountability of task at services na kailangan nilang maibigay sa tamang oras at kailangan nilang managot kung ito ay di maibibigay sa tamang oras at ang kalidad nito ay kailangang panatilihin. Kaya ang bawat Health Care infrastructure ay kailangang magkaroon ng kakayahan upang mabantayan ang kailangang impormasyon upang magawa ng Primary Care Provider na masuri ang kanyang Care network. At dahil ang Care network ay lumalago at ang interaksyon sa pagitan ng network care providers ay tumataas ang Health Care infrastructure ay kailangang maging epektibo sa pagtupad pagbabagong ito.

Ang sikreto sa mataas na mabilis at hiwahiwalay na Care Management system ay ang peer-to-peer architectural framework. Ang framework na ito ay ginamit na sa maraming industriya gaya ng, media, sports, real estate, supply-chain, paglalagay ng blockchain ay madaling idagdag sa software connector sa umiiral na centralized frameworks. Ito ay nagturo sa atin upang gamitin ang block chain framework dahil ito ay pwedeng gamitin upang mabuksan ang peer-to-peer framework para sa healthcare.

Ang Block-chain ay nangangakong susuriin ang dalwa o higit pang entities na kalahok sa "healthcare transaction". Ito ay magbibigay ng two key attributes kumpara sa centralized authentication model. Una, ang sinumang interisadong partido ay maaaring makipagugnayan sa isa't isa sa "transaction level" ng "trust relationship". Pangalawa, ay ang liability exposure dahil ang relasyong ito ay limitado lamang sa "transaction level" engagement. Ito ay kagamit gamit dahil nililimitahan nito ang pagkuha ng impormasyon at pananagutan sa bawat isa, habang pinapahintulutan nitong na makapag ugnayan sa marami pang providers base sa kanilang ispesipikong kakayahan at uri ng kanilang serbisyong binibigay sa pasyente. Ito ay mas maganda kaysa sa conventional centralized systems na limitadong bilang lamang ng providers ang pinapahintulutan para sa maraming pangangailangan ng pasyente dahil sa kailangang gawin upang magamit ang access and liabilities.

3.6 Health Information Exchange at Tokens

Ang Patientory token (PTOY) ay kailangan upang mapagana ang blockchain infrastructure. Ang talagang gamit ng the token ay upang balansehin ang network storage allocation, health care quality measures at revenue payment cycles.

Ang pasyente ay binibigyan ng tamang dani ng espasyo para oailagay ang kanilang impormasyon ng libre sa Patientory network. Pinapayagan ng PTOY na bumili sila ng extra storage space mula sa nodes set up sa hospitals systems. Ang PTOY ay maaaring bilhin gamit ang platform o pakikipagpalitan.

Ginagamit din ng mga Healthcare organizations ang PTOY sa ganitong paraan. Ito rin ay ginagamit sa pagbabayad kapag ang smart contracts ay nagamit

kasama ang healthcare insurance companies at magsisilbing mekanismo upang magtakda ng halaga nito base sa model metrics.

Upang makaalis ang US sa fee-for-service model papunta sa ngayong value-based model, ay nangangailangan ito ng healthcare IT infrastructure na papahintulutan ang ang mga organisasyon upang bumuo ng maganda, may halaga at epektibong medical interventions gamit ang reputable compensation model.

Ang benepisyo ay base sa kung papaano naging mas epektibo ang trabaho nghe network of providers ng magkakasama upang mapanatili ang pagbabago sa kalidad ng pagaalaga at paggaling ng mga pasyente habang binabawasa ang mga gastusin patungkol dito. At upang mas lalong bigyang benepisyo ang mga lalahok sa network upang makagawa ng mas magandang care regimes, isang merit based compensation ng shared savings (reimbursements) ang gagawin. Para malagyan ng tamang alokasyon ang mga provider sa network na na tumulong sa overall savings, ay maayos na tracking ng kanilang kontribusyon ay masusukat gamit ang smart contracts sa blockchain network .

Ang iba pang pagbabago sa healthcare paradigm ay ang compensation model na kung saan ang providers ay maaaring tumanggap ng karagdagang kabayaran. Ang bayad na ito ay resulta ng ipon na nagawa base sa kung papaano naging epektibo ang mga provider sa pagaayos ng kalusugan ng kanilang patient's health outcome (incentives). Ang anumang ipon na nalikha gamit ang ganitong pamamaraan ay maaaring maiwan sa mga providers at sa kanilang network partners bilang shared savings aspect ng bagong healthcare paradigm.

Ang aming proposal ay nagbibigay kakayahan sa payors upang maglipat ng tokens bilang incentives sa providers na nakagawa ng mga quality metrics. Ang kakayahang maaring humanap at magayos ng smart contracts na kung saan ang mga benepisyo ay maaring matanggap ng maayos ay nagbibigay ng inspirasyon at lakas para sa mga providers at patients upang aktibong makiisa sa symbiotic collaboration. Sa kabaligtaran, kung may isa o higit pang participants ang hindi makasunod, sila ay bibigyan ng karampatang kaparusahan at pwedeng bawiin ang anumang ibinigay sa kanila. Itong "carrot/stick" approach ay magbibigay ng inspirasyon upang mabago ang healthcare industry mula sa sickness management mindset papuntang wellness lifestyle mindset.

Kaya ang Patientory ay nag labas ng tokens (PTOY), ito ay native token para sa Patientory platform. Kapital ng PTOY tokens, ang users ay maaaring gumamit ng network upang rentahan ang health information storage space, at upang gawin ang health specific smart contract payments and transactions.

Kami ay lubos nananiniwala na ang paggamit ng token ay isang magandang paraan upang masuportahan ang infrastructure para sa hinaharap. Ang hinaharap ay maaaring magiging panahon ng maraming tokens, na kung saan ang healthcare ay kailangang makasunod. Ang resulta ay magiging mainam na cycle management positive feedback loop na may mas mababang healthcare payment fraud na umaabot sa bilyong dolyar [4].

Ang sistema ay binibigyang benepisyo rin ang mga malalaking organisasyon na may sapat na server storage para maipangalakal ang tokens na may maliit at may kalakihang healthcare organizations na nangangailangan ng direktang access sa blockchain health network na hindi kailangang ipatupad ang node. Kahit na ang bagong mga polisiya ng healthcare ay maaring magbigay ng benepisyo para sa mga providers upang gumawa ng magkasama upang paunlarin ang care pathways, ang kasalukuyang EHR architectures ay kulang ng ganitong kakayahan kaya ang pagbibigay at pagtanggap ng tokens ang ginagawa ng prosesong ito.

Kaya ang value of the tokens ay nakatali sa dami ng transactions na ginagawa sa network. Dahil ang Patientory network ay patuloy na tumataas sa token transactions ang demand para sa token ay tumataas, na nagreresulta sa pagtaas ng value nito.

Figure 4: Patientory Token Value as a Function of Transactions

3.7 Token Acquisition

Ang PTOY ay maaaring makuha sa pamamagitan ng Patientory's native app, crypto-currency market at mula sa ibang patient, physician o insurer via transfer. Ang mga platform users ay may kakayahang makakuha ng PTOY sa pagpapadala ng Ether ("ETH") sa gumagawa ng PTOY contract sa blockchain habang pre-sale. Ang Patientory interface ang maglalagay ng third party trading solutions gaya ng Shapeshift at Coinbase para sa users na walang ETH.

Ang unang pamamahagi ng Patientory Token ay sa pamamagitan ng presale. Kahit sino ay maaring makakuha ng PTOY sa discount rate sa paglalagay ng ETH sa token sale smart contract. Yung may ibang cryptocurrencies gaya ng ETC o BTC ay kayang gumawa ng PTOY gamit ang third-party conversion service na makikita sa pre-sale page.

Ang founding team ay makakatanggap ng 10% alokasyon ng PTOY, na kailangan ihinto muna sa loob ng 12 buwan. Ang token na ito ay magiging pangmatagalang benepisyo para sa Patientory founding team. At karagdagang 20% ay ilalagay sa Patientory Foundation fund na gagamitin para sa mga pananaliksik ang pagpapaunlad patungkol sa blockchain technology para sa gamit ng healthcare.

3.8 Smart Contracts and Insurance claim processing

A. Auto-adjudication

Ang komplikadong medical billing at proseso ng third-party reimbursement para sa pasyente ay kadalasang nagreresulta sa pagkabalisa o hindi

pagkakaunawaan sa pagitan ng pasyente at medical provider, at insurer. Ang mg kalituhang ito ay kadalasang nagdudulot sa mga consumers ng walang kaalaman sa kung kalian, sino, at kung magkano ang kailang bayarang medical bill o kung ang pagbabayad ba ay kanilang responsabilidad o sa insurance provider.

Ang patientory ay platform na ginawa upang magamit ang parehong Ethereum blockchain technologies at Fast Healthcare Interoperability Resources (FHIR) compliant application program interfaces (APIs) upang pataasin ang kakayahan nito, paganahin ang near realtime claim adjudication, at magbigay ng transparent agreements sa pagitan ng stakeholders at pababain ang panloloko.

Nalikha ang FHIR bilang industry standard na paggagayahan ng data upang mabawasan ang pagiging komplikado para sa healthcare at insurance legacy systems. Ang susi sa ating solusyon, dahil sa gastos sa pagdadagdag ng data sa blockchain, ay pagbabawas sa data sa kung ano lamang ang kailangan para sa paggawa ng smart contracts.

Ang Billing at Insurance Related costs ay tinatayang aabot sa 315 Billion dollars (USD) sa taong 2018 at ang medical offices ay uubos ng 3.8 hours kada lingo sa pakikipag usap sa mga payers, ang platform natin ay maaring magdala ng kaginhawahan sa ating operational costs.

Ang pamamaraang gagamitin sa pagtingin sa cross correlation para sa diagnostic information ay maaari ring gamitin upang suriin ang claim data para sa hindi makatotohanang bagay. Ang pagsusuring ito ay maaari ring maghayag ng Gawain gaya ng drug seeking behavior dahil sa multiple claims. Ang parehong ito ay dumadagdag ng halaga sa paggamit ng sistemang ito ng mga insurance companies, ngunit ang totoong benepisyo ay higit pa sa mga impormasyon.

Dahil sa rule based system na pinapatupad ng smart contract system, ang lahat ng sakop ng kasunduan ay pwedeng ilagay sa smart contracts na patunay laban sa mga end users. Ito ay nagbibigay pahintulot para sa medical facility upang magtannong patungkol sa sistema upang suriin ang sakop nito bago ang pagbibigay ng serbisyo. Ang paggamit ng sistema upang paglagyan ng impormasyon ay pinapayagan din sa automatic billing sa pagitan ng institution at ng indibidwal bilang pagkakautang na token. Kaya ang institution at ang indibidwal ay handa nang malaman ang kanilang ginastos. Tinatanggal nito ang maraming trabaho mula sa accounting departments, at dinadagdagan ang halaga ng system adoption.

Dahil dito ang Patientory ay closed loop payment system. Inaasahan na ang cross chain linking ay papayagan para sa ligtas na palitan ng halaga gamit ang public Ethereum Blockchain. Ang mekanismong ito ay naayos na para sa negosasyon ng transaksyon ng Bitcoin, kahit na ito ay nangangailangan ng pinagkakatiwalaang entity na kikilos bilang Oracle.

B. Feasibility

Sa pamamagitan ng umiiral sa mekanismo, ang arketekturang ito ay maaari nang gawin. Isang halimbawa ay ang pagkonekta ng Amazon Web Service's HIPAA compliant data storage system sa madaling isamang ErisDB. Ang SAAS ay

pinapahintulutan ang mabilis na pagpapakalat ng Ethereum smart contract capable blockchain na may buong pahintulot upang makontrol ang mga nabanggit sa itaas. Ang pagdadagdag ng passive nodes ay nangangailangan magawa, ngunit ito ay maliit na gastos lamang sa pagpapaunlad ng kompletong arkitektura.

Sa three-tiered Smart Contract architecture ng Patientory, ang subset lamang ng smart contract ang ginagamit sa Ethereum blockchain. Ang komplikadong business logic ay inalis sa execution path, na pinapahintulutan ang data tier upang magamit ng mahusay upangipakita ang pagkakahati ng nature of the network.

Ang nilalaman ng smart contract package na ginagamit sa Ethereum blockchain ay isang database schema, ang validation at verification ng transaksyon na nakalagay sa ledger, at query optimization logic para sa pagbasa ng ledger.

Ang business logic ay kinukuha sa taas ng Ethereum blockchain para maghiwalayin ang gitnang (business) layer. Ang logic codeay pinapasok ang maraming services, kasama ang secure execution, attestation, identity, cryptographic support, data formatting, reliable messaging, triggers, at ang kakayahang pagsamahin ang code na iyan sa schema sa ispesipikong smart contracts sa anumang bilang ng blockchains, na nagpapahintulot sa Patientory para magamit sa maraming grupo ng healthcare. Ang serbisyong ito ay nasa fabric, na ang bawat codes na sumusuporta sa smart contracts ay maaaring gawine, magpadala ng transaksyon sa blockchain nodes, at maging and sakto sa schema na nasa data tier.

3.9 Additional Unique Benefits

Kahit na ang mga medical institution, gaya ng hospital ay hindi maaaring pahintulutan sa anumang records na hindi pa pinapayagan, sa pagpapahintulot ng users sa pagbibigay ng impormasyon sa panahong talagang kinakailangan, ang end user ay maaaring magkaroon ng karagdagang benepisyo mula sa pakikilahok sa mga serbisyo. Dahil dito ang pangangailangan sa medical facility upang ma-access ang mga records ng mga walang malay na tao sa emergency ay bumubuo ng sitwayon na nagpapahintulot na mabukasan ang kanilang impormasyon dahil dati na nila itong pinahintulutan. Kung sakaling ang tao ay walang malay at nasakanya ang kanyang cellphone, ang institusyon ay maaring patunayan ang kanyang pagkakakilanlan gamit ang secondary signature method na nasa kanyang lock screen ng kanyang smart-phone. Ang pangalawang key ay hindi dapat parehong private key sa kanyang primary account. At kung ang institution account ay magpasa ng request sa blockchain na naglalaman ng public key ng indibidwal at ng smart-phone ng indibidwal ay pinasahan ng emergency signature, ang blockchain ay maaring pagbigyang makakuha ng medical records na hindi nito pinapayagan nung una. **Ang private key na ito ay dapat burahin din at palitan ng indibidwal ng maaga. Dahil dito ang ligtas**

na pagpapalitan ng impormasyon sa pagitan ng indibidwal at ng authorized institution ay maaaring gamitin sa emergency conditions.

Kapag ang institution ay humingi ng impormasyon ng walang tamang authorization, ang indibidwal ay padadalhan ng abiso sa ginawang aksyon. Kapag ito ay hindi pinahintulutan ng indibidwal sa tamang oras, ang data ay hindi ibibigay. At kung susubukan ng institusyon ay susubukang kumuha ng impormasyon ng paulit ulit nang hindi pinahintulutan sila ay paparusahan ng pagtanggap ng kanilang pribelehiyo, monetary punishment, at legal actions. Ang pagkasirang naidulot ng pagkawala ng cellular device ay maliit lamag dahil sa pangangailangan ng parehong cellular device at institution level key. SA hinaharap, lahat ng insurance cards ay maaaring maglaman ng cryptographic micro-controllers, gaya ng sa mga bagong credit cards, na kayang nang gamitin ng walang smart phones.

4 National/International Health-care Priorities

4.1 Personalized Care

Upang makamit ang pinaka magandang epektibong pag-aalaga, ang person centric approach ay mahalaga. Ang approach na ito ay kailangang masusing tignan hindi lamang sa clinical na aspeto nito kundi sa social at economic factors din na pumipigil sa kakayahan nitong maayos na makasunod sa care compliance at malusog na pamumuhay upang makamit ang magandang kalusugan.

Upang makamit ang inaasahang epektibong pangangalaga, ito ay nangangailangan ng malinaw na pagaalam sa mga humahadlang sa malusod na pamumuhay ng indibidwal. Sa lumalaking bilang ng pasyente na may 2+ co-morbidities, ang “siloed” one-type of care fits-all care delivery approach ay hindi magandang motibasyon upang lutasin ang care outcomes. Kaya ang isang mas flexible na care model na ginawa para isama ang multi-faceted na kalusugan ng pasyente at ang iba pa nilang pangangailangan ay kailangang makosidera. Ito ay nangangailangan ng comprehensive, dynamic interactive care plan na kung saan ang mga pasyente ay maaring makita, maayos, at makilahok sa pangangalaga sa kanilang kalusugan.

4.2 Clinical Outcomes

Ang patient-related outcome measures (PROMs), na sumesentro sa resulta na direktang tumutukoy sa pasyente, at nagkaroon ng importansya at kabuluh sa loob ng nakaraang mga taon. Ito ay nararapat para sa mas mataas na atensyon sa karanasan ng pasyente at upang magbigay ng patient-focused assessment sa bigat at hirap ng kanilang sakit. Ang PROMs ay maaring maglaman ng mga sintomas ang iba pang aspeto ng magandang kalusugan na magiging indiksyon kung physical o social function, treatment adherence, at satisfaction with

treatment. Maari din silang magbigay ng mas tamang patient-physician communication sa bigat ng treatment-related morbidities sa pagbibigay ng mas detalyado at kompletong ebaluwasyon ng paggagamot para sa ispesipikong kundisyongaya ng cancer o multiple sclerosis.

Ang PROMs ay naiiba sa traditional clinical efficacy measures (e.g., survival in cancer, smoking cessation) dahil direkta nitong nilalagay ang epekto ng sakit at maaaring paggamot dito mula sa pananaw ng mga pasyente. Ang paraang ito ay maaring masuri ang balanseng pagtingin sa pagitan ng kaayusan ng paggagamot at ang epekto nito sa pasyente. Ito rin ay epektibo sa pagtingin ng mga areas gaya ng physical functioning at overall well-being, at pagbibigay diin sa epektibo at ligtas na pagbibigay lunas kaugnay ng pangkalahatang clinical benefit. Dahil ang pamamaraang ito ay pinaunlad mula pananaw ng pasyente, ito ay magbibigay din ng mas malaking partisipasyon ng pasyente sa kung ano ang paggagamot sa kanya at upang mabigyan sya ng malinaw na ganbay sa kanyang kalusugan. Mahalagang malaman na ang pagpapatibay sa blockchain PROM infrastructure ay pagpapatibay din sa kakayahang bigyan ng magandang benepisyo ang mga providers at payors sa pagsunod sa care standards.

5 Conclusion

Ang blockchain ay magkakaroon ng mahalagang parte sa healthcare IT at magdadala ng mga bagong banepisyo at mga bagong kaunlaran sa lahat ng stakeholder sa ecosystem. Mahalagang bagay na ang mga healthcare organizations ay naiintindihan ang pinakang nilalaman ng blockchain technology upang sila'y maging handa sa mga pagbabago sa makabagong teknolohiya.

Ang resulta ay isang makabagong henerasyon ng malalakas na blockchain-based applications na babago sa kalagayan ng mga healthcare business. Upang makamit ng blockchain ang totoong potensyal nito sa healthcare, it ay kailangang naka base sa panuntunan upang masiguro ang compatibility at interoperability sa loob ng 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 itcomputable 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/healthcare-anti-fraud-resources/the-challenge-of-health-carefraud.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 networkbased 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/specialtopics/de-identification/index.html#protected>. [Accessed:04Apr-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..