The Missing EMR Cornerstone: Securing HIPAA Permissions on the Blockchain

Charles S. Kaplan, M.D., C.M.D
July 29, 2016

Abstract

Electronic Medical Record (EMR) interoperability, the ability to share and aggregate medical information securely and in a timely manner, has proven to be a persistent ongoing problem for the health care industry. In this paper, a specific implementation for improved interoperability is presented, in which the focus changes from an EMR-centric permissions model to a patient-centric permissions model. The implementation leverages and preserves existing health information infrastructure, including existing private EMR vendors, EMR portals, state-based Health Information Exchange (HIE), and the Open Authorization Protocol (OAuth). However, the new model implements blockchain technology to create an encrypted, globally accessible ledger of who has delegated permissions to whom. It is demonstrated that the flow of permissions delegation in this model more accurately mirrors the purpose of HIPAA, which focuses on the patient's intent. It also has the capability of improving the quality of care while reducing the costs. It allows for highly specific, granular control of permissions at the local level, and can form the foundation for multi-state and even national interoperability at the point of care.

Introduction

EMR Vendor Infrastructure. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted by Congress and signed into law on February 17, 2009, was designed to stimulate the adoption and meaningful use of health information technology. It offered financial incentives and stimulus funds directly to healthcare providers for adopting EMR technology, and also tied meaningful use of the technology to CMS reimbursement. Numerous private EMR vendors are competing independently to develop implementations and tools to meet the rapidly changing requirements for meaningful use. Although there has been substantial consolidation in the industry, medical data at the point of care is still organized into individualized silos specific to the provider of care, such as hospital, outpatient laboratory, outpatient imaging center, primary care office, specialty office, etc., and within each category of provider there are multiple competing vendors.

HIE Infrastructure. One of the key criteria of meaningful use is the ability to share data electronically between providers and vendors. With this in mind, on August 20, 2009, the Office of the National Coordinator for Health Information Technology (ONC) issued funding for states to set up individual state-based HIE programs. All 50 states have participated, but some states have experienced minimal to no adoption rates at the point of care. Similarly, exchange of data between states varies greatly and has not been standardized. There has been no significant progress made to initiate a national, unified HIE to date. In addition to the state HIE's, private vendors have offered HIE services to entities in geographic regions, based on markets and leverage. Many of the private

HIE's are extensions of existing EMR vendors with substantial market share, but have not achieved universal connectivity.

Portals. Direct electronic access to Protected Health Information (PHI) is done via portals for patients, and via EMR user log in for providers. Permissions for access are managed by EMR administrators. In the case of health care providers, the EMR administrator authenticates the identity of the provider and issues a user ID. The provider then selects a password, and then the provider is able to log in directly to the EMR server specific to one vendor, via either a browser or a thin client. From this point, the provider can select the record of the patient being treated and both view data and enter data. Generally, only one patient can be accessed at any one time, and providers using multiple EMR vendors at different sites can only access one vendor's record at a time on an individual patient. A more limited portal is also provided to patients for their own personal use. Again, permissions for access are controlled by EMR administrators. For patients, enrollment is usually initiated by an email invitation by the provider, and that invitation serves as authentication of the identity of the recipient. The recipient (patient) then navigates to the web-based portal via a browser, and either is authenticated by a portal-specific password that the patient selects, or is authenticated using the Open Authorization Protocol (OAuth), which allows the patient to use credentials from a third party such as Facebook or Google to verify identity and log in (Hardt, 2012). From there, the patient can view a subset of his or her personal medical record database, and also generate and receive messages to and from the associated provider. Again, the patient only has access to one EMR at a time. Patients with multiple providers (hospital, lab, primary care, specialist) with separate EMR vendors will have a separate portal, and a separate log in, for each provider.

Identification of the Problem: The EMR-Centric Permissions Model

The Health IT infrastructure described above can be summarized as being the EMR-centric model of healthcare permissions. Permissions for accessing PHI are granted by the EMR administrator to either the provider, or to the patient, or to both independently. There is no provision for delegated permissions. In other words, it is not possible for a patient or a provider to directly and electronically delegate permissions directly to a third party, such as another healthcare provider, a guardian, a pharmacy, a home health agency, a skilled nursing facility, a hospice, an ancillary provider. This creates a lot of redundancy throughout the system, as all of the providers involved in the care of a patient attempt to collect the same PHI independently of one another at the point of care. There are frequent duplications of records, errors of commission or omission, and there is no easy way to reconcile all of these records at the point of care. The best attempt for reconciliation of discrepancies is via data that is shared via the HIE mechanism in place. However, the format of this information is different from state to state, and from vendor to vendor, and many connections do not exist, particularly between the smaller vendors. In practice, most shared EMR information between systems is still done via paper records and faxing of images of documents. This model results in unnecessary delays, gaps in quality of care, and increases in costs.

Solution Overview: The Patient-Centric Permissions Model

HIPAA allows patients to delegate permissions for access to PHI to multiple healthcare providers, personal caregivers, family members, facilities such as hospitals and imaging centers, and to legal guardians and other proxies. HIPAA also allows providers to delegate permissions for access to PHI secondarily to other specific providers involved in the care of a patient, or to query for PHI in emergency situations. HIPAA also allows patients to revoke access to PHI in certain situations, such as a change in provider, or a change in legal guardian. Therefore, a permissions model that more closely mirrors the intent of HIPAA, and allows for HIPAA-compliant delegation of permissions, would allow for a more timely and effective flow of information, and would improve the quality of care. A model for permissions management that is patient-centric is proposed, and further, it is proposed that a ledger for delegated permissions be created, and be encrypted to protect privacy and maintain HIPAA compliance, while at the same time be universally available at very low cost, on a public, distributed network of nodes.

Proposal for a Blockchain Ledger for Medical Permissions Management

Blockchain Technology (BT) has a unique set of characteristics that lends itself well to the patient-centered model. BT allows for the generation of unique public/private key pairs that can be bound to an individual's identity. BT is available as open-source software, that can be modified to suit any particular use case, and be specialized for specific tasks. BT allows for the creation of long-term, stable distributed networks of nodes that can share information and authenticate information very quickly. The data stored in Blockchains can be accessed by any existing application through the use of an application programming interface (API), allowing for the creation of customized user interfaces. Blockchains are ideally suited for creating a distributed ledger of timestamped transactions between clients. An important point to stress is that in each and every transaction on the blockchain, there is a space reserved for data, such as a message, in addition to the transaction itself, and the data becomes accessible to the network.

A blockchain-based ledger can be implemented in healthcare practices as follows: first, a peer-to-peer network of nodes is set up. To ensure that network is always maintained, a set of nodes is designated by a healthcare organization to be committed to be online and connected to the network 24hrs per day, seven days per week. Typically, these nodes could be run on existing healthcare servers or other designated machines, distributed over a wide geographic area. Then, individual patients and providers are able to freely connect and disconnect to the network as needed, using PC's, laptops, tablets, phones, or other mobile devices with network connectivity. A single ACO could set up a blockchain network, or it could be statewide, national, or even global.

Each patient and each provider using the blockchain would connect to the network using a client application analogous to a cryptocurrency wallet. The client app connects to the network of nodes and synchronizes to the distributed blockchain. However, instead of sending and receiving financial transactions, the client app would send and receive HIPAA permissions transactions. This type of a blockchain can be designated as a "Medical Permissions Blockchain", or MPB. In the

next section, the nature of a Medical Permissions Blockchain is described in more detail, with some pertinent background information.

Medical Permissions Blockchain (MPB) - Additional Details

Blockchain. A blockchain is maintained by a network of nodes, and each node contains a private account. Each private account is secured by a public/private key pair. Only the possessor of the private key can access any given account. Communication between nodes can occur in the form of transactions, that are initially broadcast to the entire network instantly, and then confirmed mathematically by a hashing algorithm. The algorithm collects a number of broadcasted transactions during a block interval, creates a new block out of those transactions, and by discovering the next mathematically optimal hash associated with that block, confirms the entire block and adds it to the chain (Patel, 2014). The average time it takes to create each block, and therefore confirm each transaction, is called the block time. The average block time can be set at the time of the launch of the blockchain. In the case of Bitcoin, the average block time is 10 minutes, and assuming the need for 6 confirmations (to be sure that the confirmed transactions are permanent, and not on an errant orphan chain), final confirmation of a transaction typically takes one hour. Multiple alternative blockchains have been started with shorter block times. For example, Syscoin, which is a fork of Bitcoin, and is therefore an entirely separate blockchain, has an average block time of 60 seconds (Wasyluk, 2016). For the MPB model, a fast block time is recommended for point of care workflow.

Blockchain keys and addresses. Each individual blockchain account is associated with at least one public/private key pair. Key pairs can be generated deterministically from the private key. A private key can be generated randomly, and series of mathematical operations can be performed on this key to generate the public key, and then an additional series of operations can be done to generate the public address from the public key (Bitcoinwiki, 2016). The public address is used to route the transactions to the correct account. The public key is revealed to the network when the account initiates a transaction. The private key is not revealed at all. The public/private key pairs are of sufficient cryptographic strength to be used for X.509 digital certificates, and for Secure Sockets Layer (SSL) /Transport Layer Security (TLS) encrypted communication (Khovayko, 2015), which are requirements of the HIPAA security rule for safeguarding PHI (HHS, 2016).

Transactions. Transactions can contain a number of elements. In cryptocurrency blockchains, one element is the transfer of ownership of digital assets, or cryptocurrency, from one account to another. Another element can include digital fees, again in the form of cryptocurrency, to distribute to the nodes in the network that did the work to process the transaction. Other elements include a time stamp, and data inside a data slot, which can be encrypted. Accounts can be created and used by patients, providers, hospitals, ACO's, health portals, EMR's, HIE's, and health insurance plans on the MPB.

Open Authorization (OAuth). Patient Heath Portals allow individual patents to individually access portions of their EMR records. When a patient logs in for access, authentication of identity is required. One such method that is commonly used is the Open Authorization Protocol (OAuth), in

which a patient logs in using his or her social media user ID and password, such as Facebook. This provides a convenient way for patients to log in, as they can use an existing secure password without learning a new one. This improves portal utilization rates for patients, and enhances portal metrics for providers.

As a general overview of how OAuth works from the user's perspective, the user browses to the Portal first, and is presented with an option to log in using one's social media credentials. The user is then redirected to the social media site and logs in. The social media site then presents the user with an option to allow, or not allow, the use of credentials to log in to the portal. If the user selects yes, then the user can use the social media credentials to log in to the health portal from that point forward.

What is happening beneath the surface is a series of handshakes between the Portal and the Social Media site, involving the exchange of keys (Hardt, 2012). This is necessary because the Portal needs to be able to verify the identity of the Social Media site itself, to prevent fraudulent access. Likewise, the Social Media site also needs proof of identity of the Portal Site, to prevent a data breach. After these confirmations have taken place, and the user has both logged in and confirmed the intent to share log-in credentials, an access token is created that allows the user to access the protected health information inside the Portal in the EMR.

Using the Blockchain for Open Authorization in a Portal

It is possible to use the proposed Medical Permissions Blockchain model in place of the social media site in this construct; essentially, allowing a patient to log in to a personal health portal using credentials stored on the blockchain. In this case, the Portal would have an account on the blockchain with public/private key pairs. By virtue of creation of this account, the series of handshakes described above is complete. The Portal can now do something analogous to OAuth: it can send an encrypted access token to the patient's account inside the data slot of a blockchain transaction. The patient is now able to use the access token to log in to the health portal, analogously to having signed in using OAuth in conjunction with a social media site.

Having the access token on the blockchain is very advantageous, because it can be delegated to selected HIPAA-authorized healthcare providers without divulging it to anyone else. This can be accomplished within the patients account, by re-encrypting the access token with the public key of the new recipient, and sending the data to the new recipient's account via a blockchain transaction.

Real World Workflow Examples

Placing HIPAA-compliant permissions in an encrypted form on a universally accessible, distributed blockchain ledger will result in profound improvements in work flow, during delivery of healthcare services to patients. To illustrate this, a number of work flow situations are enumerated below to contrast blockchain vs non-blockchain permissions management.

The New Patient Encounter. The current practice is for new patients in a medical office to attempt to recreate their entire medical history, to the best of their ability, without medical training, on questionnaire forms. After that, a release is signed, and medical records are requested via fax. Records may appear in a few days via fax or mail, or via computer disc, to be scanned and imported manually. Sometimes, a Summary of Care is generated after these requests, after a delay of time, typically hours or days, and then is transmitted to the new practice via the state HIE. In contrast, with Medical Permissions Blockchain (MPB), the patient arrives, sends a permissions transaction to the provider using his or her own mobile device, the transaction is confirmed in sixty seconds, and the new provider has access to any previous healthcare portal that the patient included in the transaction.

Referrals. Up to this point in the discussion, the patient has been the one cited as sending permissions transactions to a provider. In the real world, it is frequently healthcare providers who are making HIPAA decisions as the patient's proxy. One example is the medical referral to a specialist, from one provider to another. Currently, when a referral is made, it is accompanied by a faxed copy of the most recent pertinent medical records, or by a Summary of Care document transmitted by the HIE. In both of these instances, the information transmitted is frequently incomplete, resulting in follow up man-hours to track down the relevant information that the specialist needs. In contrast, with MBP, the referral is done with a single permissions transaction, and the information available to the specialist via the patient's heath portal(s) will be more complete from the outset. When the referring provider has access to more than one of the patient's portals, additional transactions can be sent to allow the specialist to have access to multiple portals belonging to that patient. The breadth and depth of medical information available to healthcare providers would be greatly enhanced, and still be HIPAA-compliant.

Laboratory and Imaging Ordering. In current real world clinical practice, when ordering laboratory tests, or imaging studies, the provider writing the order does not alway have access to all of the pertinent past lab or imaging data, which may affect the ordering decisions. With MPB, it is more likely that the ordering provider will have access to all of the pertinent information, because when providers involved in the care of a patient also delegate permissions to the appropriate portals, lab and imaging results from multiple portals can now be consolidated electronically at the point of care.

Revoking permissions. Patients have the right under HIPAA to revoke permissions for access to protected health information, moving forward, from providers or caregivers who had it previously. This sometimes occurs when a change of provider or caregiver occurs. With the MPB model, this is accomplished by the patient requesting a new access token from his or her portal, and then sending transactions with the new encrypted access token to the new panel of care providers. The old access token will no longer be valid at the level of the portal.

Emergency care. Currently emergency services are often provided in the absence of prior medical records from outside the hospital system. If a patient presents for emergency care and is conscious, one MBP transaction would give the emergency provider immediate access to records. Let us consider the instance in which a patient presents for emergency care, and is not conscious. There is

a way to provide the emergency providers with immediate access to medical records using MBP. This is possible because the patient's own blockchain account can be created deterministically from a given private key, and when setting up the account, this private key can be purposefully generated as a hash of combined biometric and personal information. It would not be possible for anyone to access the individual's account unless they had access to the biometric information and the personal information at the same time. In this example, the private key is a hash of the fingerprint of the patients left third finger, combined with the health insurance ID number. Even if the patient is unconscious, emergency healthcare providers would have access to the fingerprint and the health insurance ID number, and could access the patient's record via the blockchain, generate the transaction to transfer permissions as the patient's proxy, and move forward with the information.

Security, Risk Analysis, and Mitigation

The example presented above raises the issue of security, and the risk of unauthorized access to protected health information. First, one must compare the proposal to the security in place today. Today, the only protection against unauthorized access to patient health portals is a password. Passwords can have various strengths, and it is well known that weak passwords are frequently chosen by members of the public for sensitive personal data, and the weaker the password, the easier it is to gain unauthorized access via brute-force attacks. Also, a number of instances of data breaches with stolen passwords have been reported, and with shared passwords, the risk of breaches goes up even higher. Compare that to the proposal to use a combined hash of a fingerprint and a personal identifier, which is essentially two-factor authentication. It is not foolproof, but it is more secure than what is in place now. In addition, patients can opt out of biometric generation of the private key, and choose random private key generation instead. The only loss of functionality with opting out is with emergency services when unconscious. Most health care encounters would still achieve all of the benefits of MPB with a random private key. A random private key would provide the highest level of security and privacy.

There are additional ways to mitigate against the unauthorized use of a biometric marker. One is to choose a marker that is not generally accessible. Instead of a fingerprint, an infrared palm vein scan could be selected (Shahin, et al., 2008). However, this would result in some substantial equipment costs, as compared to the presence of fingerprint scanners in many current personal handheld devices. Another strategy would be to choose a different biometric marker and a different personal identifier for each patient, and store that meta-information elsewhere. Strategies would have to be developed to allow emergency personnel access to the meta-information in a timely manner.

Costs and Implementation

There will be costs to implementing the MPB model. Although current EMR and HIE infrastructure can remain largely intact, enhancements to patient portals will have to be made, to allow for the Open Authorization protocol to be adopted to the blockchain. Fortunately, there is precedent for Open Authorization to be utilized by portals, as OAuth has previously been

implemented by EMR patient portals for Facebook, Google, Yahoo, Microsoft, and other parties. However, the overall cost of implementing MPB is greatly reduced, compared to alternative universal identity and permissions protocols, by the open-source nature of blockchain technology. The API to access the blockchain is also open source. This greatly reduces licensing fees and also opens the door to competition from third party developers. This may ultimately drive the cost of EMR software down, saving the overall healthcare system significant funding.

Initially, implementation should focus on patient portals, however, in the long run, it would be useful to have dedicated provider portals, either to individual EMRs or to HIEs. Again, third party vendors may wish to develop these and have them certified by ONC. One of the most significant costs is the initial certification, and maintenance of certification, for HIPAA compliance, of the software. Existing EMR vendors, or state HIEs, may be best positioned to incorporate these portals into their legacy systems, as they already have the certification infrastructure in place. Consolidation of portals for simultaneous access to multiple EMRs, or simply directly to state HIE's, would result in cost advantages and increased ease of use (Mohan, 2016).

An important consideration is the selection of which blockchain to use. There are many options, such as whether to start a dedicated blockchain solely for the purpose of MPB, or to utilize an existing blockchain that is already established and being used for commerce, or other purposes. It is probably premature to select a specific blockchain at this time, but pilot studies could be done with the best existing candidates, and performance could be compared. Examples of current blockchains that are early in development, but have encrypted messaging capabilities for MPB are Syscoin, Emercoin, Ethereum, and Lisk.

HIPAA also specifies that PHI permission control should be granular. For instance, patients can grant permission for access to most healthcare data, but can exclude specific portions from disclosure, such as behavioral health data, or HIV status. Also, HIPAA provides for disclosure of de-identified PHI to administrative entities such as ACO's for metrics. To allow for granular control of permissions on the blockchain, each MPB transaction can include in the data slot not only the encrypted access token, but a code to specify the specific set of PHI being disclosed.

Implications for the Nationwide Interoperability Roadmap

The Office of the National Coordinator for Health Information Technology has published a Nationwide Interoperability Roadmap, entitled "Connecting Health and Care for the Nation" (ONC, 2015). The document lays out specific goals and timeframes for our country, including the goal of "achieving nationwide interoperability to enable a learning health system, with the person at the center of a system that can continuously improve care, public health, and science through real-time data access" by the years 2021-2024.

The past decade of rapid health information system expansion has been an instructive experiment, with both major successes, and shortcomings. What has become evident is that the current procedure for managing HIPAA-related permissions has proven to be a major stumbling block to effective interoperability. A new system that models itself directly on the intent of HIPAA, which

is to allow patients to directly delegate permissions to caregivers, and to allow caregivers to act as proxies when appropriate and secondarily delegate permissions, will serve as a powerful foundation for health IT moving forward.

Up to now, medical permissions have been granted, and validated, on paper HIPAA release documents. The authentication is the hand-written signature of the patient, and the people executing the will of the documents are clerical staff, acting under the supervision of EMR administrators. The curious fact is that now we have EMR and HIE, with medical data warehouses containing SQL files, and paper-based HIPAA-permissions translates directly to the IT world, where permissions to view data are literally SQL commands, such as the basic SQL command:

```
GRANT privileges ON datbasename, tablename TO username@host IDENTIFIED BY "password";
```

Yet we are still held back by a paper-based permissions system, and there are too many intermediaries in the process.

It is imperative that we, as health IT policy-makers, find a way to allow patients, and providers, to securely manage medical permissions electronically, in full compliance with HIPAA regulations, and with the speed and timeliness that will realize the ultimate goal of the Roadmap, which is to deliver nationwide interoperability at the point of care, through "real-time data access." A blockchain-based permissions model can be that foundation.

Summary

Clinical health information interoperability is inherently limited by the current prevalent EMR-centric permissions management model. Inverting the permissions model to a patient-centered system more closely mirrors the intent of HIPAA regulations, and allows for more timely and efficient interoperability. A blockchain-based model is proposed that leverages existing health information infrastructure, taking advantage of the best features of existing legacy EMR systems, state HIE programs, and health portals, but expanding functionality at the point of care. Health information security and privacy are maintained due to the strong cryptography utilized in blockchain technology. Several work flow advantages are demonstrated, and business opportunities are presented. Patient-centered medical permissions management, encrypted on a distributed ledger, is highly compatible with the long term goals of the ONC Nationwide Interoperability Roadmap (fig. 1).

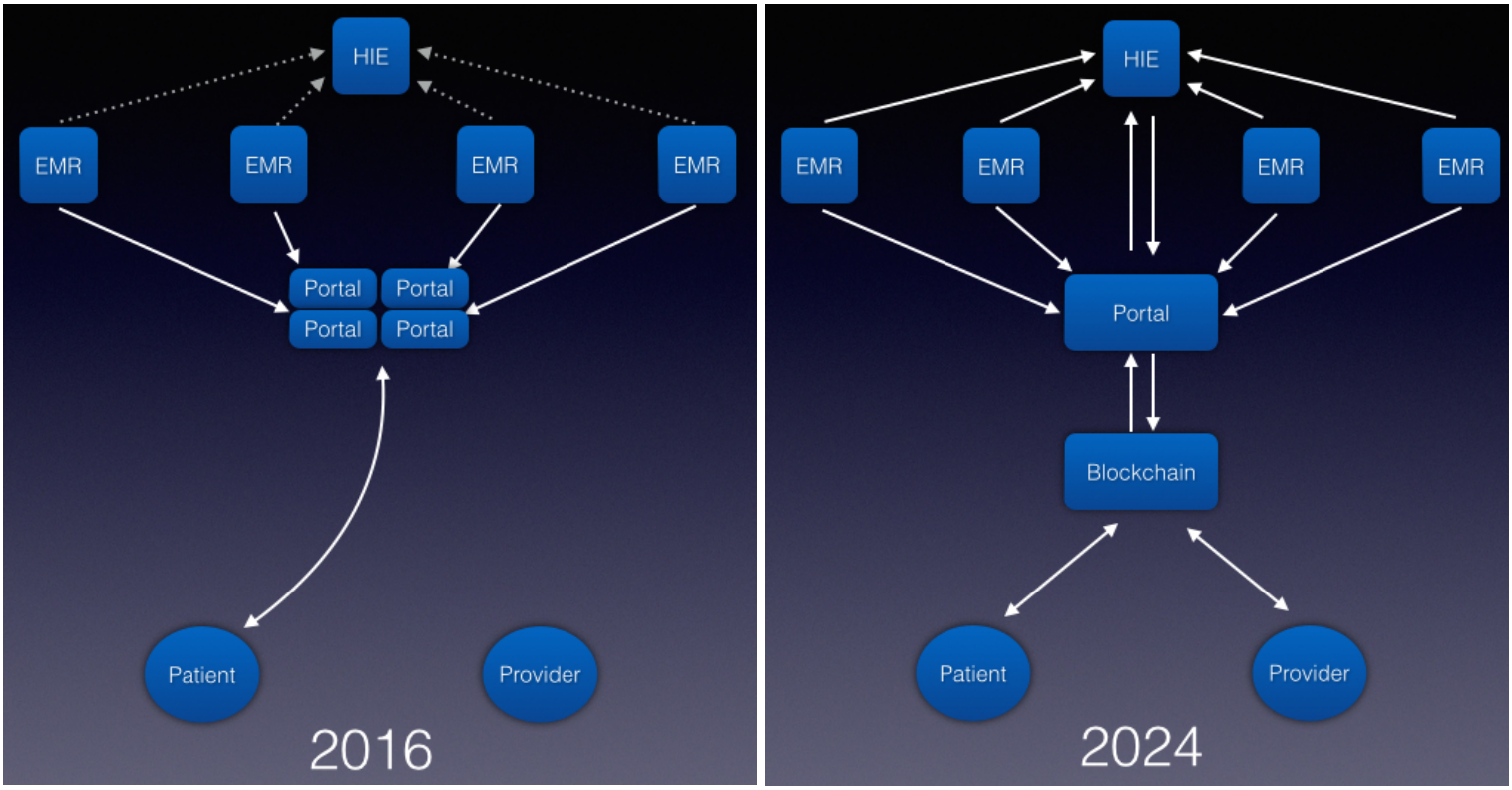

Fig. 1: The Medical Permissions Blockchain and the Interoperability Roadmap

In this illustration, currently in 2016, a patient with health records in 4 EMRs presents to a new provider. The patient has access to 4 different portals, one for each EMR. The EMRs all are enabled to communicate with the state HIE, but data transfer is incomplete. The provider has no direct access to any of the 4 portals. In 2024, the patient can delegate HIPAA permissions to the new provider using a handheld device, through the blockchain. The transaction is confirmed by the network in 60 seconds. The portals have consolidated, and communicate with the blockchain using a process analogous to OAuth. The patient and the new provider have options to immediately access all the data via the individual EMRs or the state HIE.

References

Bitcoinwiki. (2016). *Technical background of version 1 Bitcoin addresses.* Retrieved July 27, 2016 from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

Hardt, D. (2012). *The OAuth 2.0 authorization framework.* Internet Engineering Task Force (IETF): Proposed Standard. Oct. 2012. Retrieved July 27, 2016 from http://tools.ietf.org/html/rfc6749%3E

Health and Human Services (HHS). (2016). *Summary of the HIPAA security rule.* Retrieved July 29, 2016 from http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

Khovayko, O. (2015). *EMCSSL: Decentralized identity management, passwordless logins, and client SSL certificates using Emercoin NVS.* Emercoin International Development Group White Paper. Retrieved July 29, 2016 from http://emercoin.com/content/EMCSSL.pdf

Mohan, S. (2016). *Too many patient portals – what can you do about it?* HIMSS 2016 Conference and Exhibition: Transforming Health Through IT. Feb. 29 - Mar. 3, 2016. Las Vegas, NV. Retrieved July 27, 2016 from http://www.himssconference.org/sites/himssconference/files/pdf/301.pdf

Office of the National Coordinator for Health Information Technology (ONC). (2015). *Connecting health and care for the nation: a shared nationwide interoperability roadmap.* Retrieved July 29, 2016 from https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

Patel, H. (2014). *A pure block chain based decentralized exchange.* IACR Cryptology ePrint Archive, 2014, p. 1005. Retrieved July 27, 2016 from https://eprint.iacr.org/2014/1005/20141225:065012

Shahin, M. K., Badawi, A. M., & Rasmy, M. E. (2008). *A multimodal hand vein, hand geometry, and fingerprint prototype design for high security biometrics.* In December 2008 Cairo International Biomedical Engineering Conference (pp. 1-6). IEEE. Retrieved July 27, 2016 from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4786038&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4786038

Wasyluk, D. (2016). *Sycoin 2.0 faq: what are syscoin's specs?* Retrieved July 27, 2016 from http://syscoin.org/faq/