HITRD RFI Responses, March 15, 2019

ACTION ON INTEROPERABILITY OF MEDICAL DEVICES, DATA, AND PLATFORMS TO ENHANCE PATIENT CARE

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

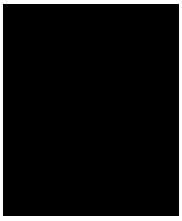
Perspectives and Visions For The Future of Medical Device, Data, and Platform Interoperability

Gracie Carter[1], Hossain Shahriar[2], Sweta Sneha[1]
[1]Department of Information Systems
[2]Department of Information Technology
Kennesaw State University
[redacted]

[redacted]**Bio - Gracie Carter:** Gracie is the Scrum Master for the Accelerator team at Sychrogenix, a Certara company. In this role she is currently managing a project for the Centers for Disease Control called OpenMDI. The purpose of OpenMDI is to streamline the death reporting process through interoperability. The accelerator team works with and draws from proof of concepts from academic stakeholders to build on as the team develops these concepts for production. OpenMDI utilizes FHIR standards for machine to machine data transfers but aims to use analytics and machine learning to allow for other, nonstandard data elements to be recognized and incorporated as well. Gracie is also a Graduate Research Assistant at Kennesaw State University focusing on interoperability using blockchain technology. She began her research into blockchain applications in healthcare in January of 2018. While pursuing her master's degree in Healthcare Management and Informatics, she has published a paper "Towards Application of Blockchain for Improved Health Records Management and Patient Care" on the subject in the Journal Blockchain for Healthcare Today. She is currently working in conjunction with public and private partners to develop an interoperability proof of concept using smart contracts, blockchain and SMART on FHIR to improve data flow with minimal intrusion on the providers workflow.

[redacted]**Bio- Dr. Sweta Sneha:** Named as one of the top Women In Technology in 2018, Dr. Sneha is the Founder and Executive Director of Healthcare Management and Informatics and a Professor of Information Systems at Coles College of Business in Kennesaw State University. She is a strategic thought leader with more than two decades of experience in technology, informatics, and healthcare. She has authored a book and over 100 research publications in high quality journals and conferences including IEEE Communications, Decision Support Systems, Decision Sciences, International Journal of Medical Informatics, International Journal of Electronic Healthcare, Journal of Global Information Management, Hawaii International Conference on System Sciences, Americas Conference on Information Systems, and IEEE Broadmed. She is a sought after speaker and has made several keynotes and participated in panels

at national and international venues including Health Connect South, TAG, International Conference on Transforming Healthcare, GLBITM Healthcare and Informatics in the 21st Century, AMCIS, HICSS. Dr. Sneha is passionate about informatics and the potential of its impact in enhancing the delivery and practice of healthcare. She is highly engaged with the community and has led projects with industry including MagMutual, Piedmont, Harbin, Wellstar, Truitt Health. She supports causes and organizations impacting workforce/economic development, education, and diversity locally and globally. She serves on multiple boards including TAG Health, Biosciences Leadership Council at MACOC, Global Health Atlanta, Fulton Science Academy, and healthcare startups Chronic Signal Inc. and Unicore. Dr. Sneha has earned many awards recognizing her work in gender equity in STEM disciplines and promoting collaborative partnerships and economic development. She has received RISE IT award from NCWIT, KSU Collaboration Award, WIT Honorees Awards, and WIT Women of the Year Finalist as one of the top three for Women in Technology for 2018. Dr. Sneha earned a BS in Computer Science from University of Maryland, College Park, a certificate in Health Informatics from AMIA, and a PhD in Computer Information Systems from Robinson College of Business at Georgia State University. She has previously worked with PriceaterhouseCoopers as a Management Consultant.



Bio- Dr. Hossain Shahriar: Dr. Hossain Shahriar is an Associate Professor of Information Technology and BSIT/BASIT Program Coordinator at Kennesaw State University, Georgia, USA. His research interests include mobile and web security, EMR and healthcare security, malware analysis. One of his research areas is focusing on automatic checking for vulnerabilities in implementation and design of applications, development of tools towards development of educational resources and capacity building on Secure Mobile Software Development (SMSD, https://sites.google.com/site/smsdproject/home), a project sponsored by National Science Foundation. He is currently investigating healthcare data interoperability issues and potential solutions, particularly adopting smart conract-based distributed apps. His research works also spanned over clinical workflow analysis, process mining, securing of Electronic Health Record Systems, smart and connected health tool. Dr. Shahriar has published over 85 peer-reviewed articles in IEEE/ACM conferences, journals and book chapters including ACM Computing Surveys, Computers and Security, and Future Generation Computer Systems. Some of his research projects have been supported by various agencies including National Science Foundation (USA), USG Affordable Learning Georgia, NSERC (Canada). Dr. Shahriar presented many tutorials on security of devices and applications including in IEEE ISSRE (2018) and ACM SAC (2016, 2015, 2014). He served as Program Chair (SIN 2016), Fast Abstract Chair (IEEE COMPSAC 2015-current), Publication Chair (ACM SAC 2017-current), Workshop Chair (IEEE STPSA 2017 - current). He is also a Symposium Chair on Smart and Connected Health (in IEEE COMPSAC 2019). Dr. Shahriar is a professional member of IEEE and ACM.

Executive Summary

The problem being addressed is how to gather information about a patient from all previous providers without an established relationship. This is achieved through publishing encrypted hashes to the blockchain with only references to the FHIR server that contains that patient's file. If the provider is able to provide appropriate key pairs, they would be able to pull and decrypt the patient file from the originating FHIR server through their SMART chain application.

Our solution proposes using a combination of available and mostly open source technology in conjunction with existing information systems to facilitate data transfer between providers while keep the cost of implementation relatively low. This scenario illustrates how blockchain can be applied in healthcare and incorporated into the electronic records management systems that providers currently using. This paper makes the assumption that each vendor will map the EMR resources to the recommended FHIR data standards. Through FHIR data standards information can be shared more freely regardless of system or device.

To ensure security, no EMR system would be exposed to the blockchain, and no complete files would be shared to the blockchain. All requests would be handled in a Smart chain application. Then pushed to the blockchain with public keys made available. No public or private keys would be stored locally. To provide another layer of security, all keys would be managed through a 3rd party key management system in the event that the EMR was compromised.

I. Introduction

The healthcare system in the United States is unlike any other. From insurance to care provider, patients have the freedom of choice. This creates a complicated and profitable paradigm of care. In this competitive privatized healthcare system, the patient is at a distinct disadvantage. Although legislation exists that clearly defines what the government expects from healthcare providers, the methods to achieve these goals are left to the discretion of the providers and a variety of vendors. Devices and programs are not built to similar standards and subsequently do not share data easily. This communication between software is known as interoperability.

II. Issues with interoperability

Among Electronic Health Record (EHR) system vendors, the most common form of information blocking was deploying products with limited interoperability. Among hospitals and health systems, the most common form was coercing providers to adopt particular EHR or Health Information Exchange (HIE) technology[1]. A survey lends credence to Reisman's [16] statement that both providers and vendors have been accused of information blocking and vendor lock-in.

Vendor lock in can be summarized as a fostered dependency on a single provider for technology and support and cannot easily transition to another provider without compromising revenue, value, and/or information integrity. Although it can happen in a variety of ways, depending on the type of product, the most common forms of vendor lock-in are legal constraints, proprietary ownership, refusal to modify to suit, competition between different vendors on the market or cost prohibitive fees associated with vendor modifications. Opara-Martins[13] mentions these barriers and adds that there is no guarantee that data can be transferred from one EMR system to another while maintaining file integrity.

Upon initial software purchase from a vendor, customers are offered incentives for vendor loyalty in future purchases. To ensure dependency, often proprietary software renders data incompatible with third-party software. This method of vendor lock-in originates and is controlled by the vendors themselves as it makes data migration an arduous task. Additionally, vendors often require that they be the sole provider of support or manipulation of the software. Also, if the customer wants part of their system modified in the future, that would require an additional purchase from the vendor. This allows the vendor to lock-in the customer for additional costs in order to update, change or maintain their software.

As technological trends are influenced by lock-in, large manufacturers are continually competing for new applications being developed for their systems. This is seen predominantly with larger named EHR vendors, compared to their counterparts. If one vendor is able to develop a new way to accomplish a previously tedious task, it becomes the shiny new toy on the market that every company and/or organization wants. The ability for vendors to market their products in this manner allows for customers to get hooked on certain aspects within the product that they love and therefore possibly diminish other aspects that may be better if they were to go with another vendor. In addition to new applications being built for these EHRs, the competition can continue with the different levels of price for features. These new features

change the code base and make it more difficult to share information with outside systems without adhering to a common data standard.

The issue is that disparate systems do not have a common language to communicate in. Using a common data standard would allow any system to map to it. Once transmitted to another point of care the information could be directed to the appropriate field in the recipient's system through mapping. The issue is not that a standard does not exist, the Fast Health Interoperability Resources (FHIR) standard has been around for several years. The issue is the lack of willingness to commit resources to share data. Through semantic interoperability if a provider becomes unhappy with their current vendor, they can move all their information over to a new vendor, at least in theory.

HIPAA states that patients own their data and should have unfettered access to them[3]. Compliance aside, many systems feel they own the data because it originated with them[10] and any patient ownership is negligible [4]. In traditional models, patients are not able to revoke access to their records. Thus, data is siloed and hoarded for permanent possession[20]. A patient may see many different doctors over their lifetime- if every provider feared to share data due to losing competitive advantage or decreasing patient retention[14] the resulting data fragmentation could leave the data vulnerable to attack[20].

Information blocking has been defined by law to be "any practice that ... is likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information"[2]. Proving intent to keep information (information blocking) is difficult to prove. Being greedy with data is not limited to systems; 49% of providers surveyed stated that EHRs routinely block information through intentionally limiting interoperability, charging high fees for exchanges, and making third party access difficult or impossible[1].

The U.S. health care delivery system continues to have a culture defined by silos, fragmented processes, different stakeholders, and competitive advantage rather than a basis for coordinated care. For interoperability to be achieved cooperation is required from providers, software vendors, patients and even legislators. In a system fraught with disparity, data becomes a precious commodity. When a business or entity controls an asset, sharing that asset could cost them potential revenue.

Currently the foundational, structural, and semantic levels of interoperability are fraught with interpretation issues. The foundational level of interoperability is the most basic in which a cache of medical records is sent (pushed) from one provider to another[4]. It is assumed that the recipient of the data received it intact and can interpret it correctly[15,4,20]. There is no accountability to this method[4]. If the interfaces do not communicate through common data models, then the data is not usable. At the structural level, records are pulled between two systems where data structures are defined[15,4,20]. In this scenario, there is no audit trail between systems[15,4,20] which allows for duplicate record requests and poses a security risk. At this level, the information is available, but not readily. Semantic is the highest level of interoperability. This would be the paramount model of effective communication. Providers would be able to view and pull the most accurate data without necessarily having an established relationship[15,20].

Non-interoperability hinders cost and quality of patient care. Without access to complete records to fully understand a patient's history, providers waste time and resources. According to the ONC a functional system should include: a secure network infrastructure, verification of identity and authentication of all participants, as well as consistent proof of authorization of electronic health records[11,12]. However, no EHR was chosen nor a requirement for interoperability was mandated. Because of legislation passed at the federal level with little strategic planning, healthcare providers at the local level adopted EHRs ad hoc to meet meaningful use. This lack of foresight coupled with a disinterest in active record management by patients has further complicated interoperability.

HIPAA was signed into law in 1996 with the intention to protect personal health information (PHI) by creating a clear directive on how to handle it while maintaining privacy through security and privacy rules. Privacy rules expressly state that all PHI must be expunged from any and all medical data before sharing it[8]. Ideally, all identifiable markers would be completely removed from records through the anonymization making all records irreversible[3,8]. This becomes a problem without a master patient index. With no clear way to identify a patient that complies with HIPAA sharing information or looking for patient data becomes so complex it isn't even attempted by most providers.

Compliance aside, many systems feel they own the data because it originated with them and any patient ownership is negligible[10]. In traditional models, patients are not able to revoke access to their records. Thus, data is siloed and hoarded for permanent possession[18]. A provider may fear sharing data due to losing competitive advantage or decreasing patient retention[14]. Beyond refusal to share, there is the issue of sharing so little information that it becomes unusable. This is difficult to prove because it is technically HIPAA compliant. Because HIPAA states that as little information as possible should be shared to protect patient data while still conveying the methods of care[1]. HIPAA is counterintuitive to interoperability through encouraging as little information sharing as possible, this equates to information blocking.

While multiple services were streamlined with the adoption of EHRs, the caveat was that these often were contained in a single health system[11]. To encourage information-transfer the 21st Century Cures Act required health IT products and services have an application programming interface (API) to allow for the use and exchange of health records and information electronically[11,7]. Additionally, these APIs must allow for health information to be accessible, usable and transferrable without "special effort", tested in real world scenarios for interoperability and be published for developers to use[17]. These requirements in conjunction with the Health Level 7 (HL7) messaging, Fast Healthcare Interoperability Resources (FHIR) standards and Representational State Transfer systems (RESTful architecture) for APIs; create working formats (XML or JSON) and architecture for healthcare data transfers[6].

III. Solution

Combination of standard data (FHIR)server, OAuth, Amazon, blockchain and smart apps. Have two Dapps, one internal that interacts with the EMR via SMART on FHIR, an EMR FHIR server, an authorization server, a key management system, a blockchain and an external Dapp that interacts with the blockchain and other providers.

To Publish: In this scenario it is assumed that each EHR would have a FHIR server set up and properly mapped to each field and SMART on FHIR. A subscription would be established with the FHIR server that sends patient source for each creation and update, without being acted upon by the provider. The file information is sent to an internal app hosted within the provider's system. This internal app extracts from the patient file their unique ID (ideally a master patient ID, but more likely a combination of Patient Health Identifier or PHI)), encrypt this information, authenticate to the blockchain, checking for existing information, if it does not exist, it is properly encrypted and publishes to the chain that a file exists using this public key with this provider.

To Request: Here, a provider would open a new window (the first Distributed App or Dapp) within the patient's file in the EHR to look for external records and provide their OpenID and the FHIR server URL. This would trigger the Dapp to retrieve the patient's metadata from the EHR FHIR server, once found this information along with authorized endpoints would be sent back to the Dapp. Using the OpenID, the Dapp would ping the EHR authentication server to retrieve the Oauth 2.0 token. This token would then be returned to the Dapp essentially allowing the process to proceed to retrieve the patient's information (ideally, a master ID from a master patient index but more likely it would be some combination of PHI). The Dapp would then interact with the key management system requesting the previously encrypted patient ID. Once that is returned, the Dapp will search the blockchain looking for potential files that reference this key. If Dapp1 (internal) interacts with Dapp2 (external), requesting all resources for the patient to be bundled. The query will be encrypted, and the public key of the provider will be shared. Once the information is received by Dapp1 (the internal app), it should be able to decrypt the file using a private key and send the results back to the EHR to display the results.

There is a need for a functional and stable solution that is both lightweight, easy to operate, and relatively quick to implement with very little user prompting. A system that requires more initial investment in infrastructure such as datacenters or a formalized IT department are prohibitive both in cost and return on investment. Data standards such and HL7 v2 and HL7 FHIR are designed to encourage interoperability through uniform data structure. This allows for systems to organize and move relevant data more quickly[6]. Additionally, having standards allows for software to be designed and developed to be interoperable across multiple platforms without extra add-ons or external programs for reconciling data structures.

Health Level 7 (HL7) is a nonprofit healthcare standard setting authority with members from upwards of 50 countries; united in dedication to creating an all-inclusive framework and standards for use in health data exchange[19]. The four focus areas for HL7 standards are as follows: version 2 and version 3 for messaging, CDA as an exchange model for clinical documents, EHR-PHR system functional models, and Fast Health Interoperability Resources (FHIR) a web-based exchange language aimed at making healthcare applications faster and easier to write [9].

The primary HL7 standard utilized for this project is FHIR. FHIR is an open-source standards framework that combines features from HL7 v2, HL7 v3, and HL7 CDA with web service technologies [6,19]. FHIR is based on RESTful web services and uses modular components

as resources [6,19]. FHIR's supported data formats are XML and JSON which are both relatively widespread and easy to convert other file types to. To add to the approachability and encourage adoption, HL7 provides an open source FHIR server for healthcare IT to use as reference to build and set up Healthcare Information Technologies that are interoperable [9].

III(A). Relevant Parties

Currently the Center for Disease Control (CDC) has undertaken a cloud-based software as a service death reporting and investigation system (OpenMDI). OpenMDI would allow for the rapid exchange of death reporting information through the use of FHIR servers and integration of 3rd party systems through the use of RESTful APIs. This model of open technology interoperability could be used across the board and since the federal government already has contracted the technology, it could be applied in other places. This model encourages data transfers between HIPAA exempt entities while maintaining security through industry standard security compliance protocols including FedRamp High and HIPAA.

Private research institutions would play a key role in furthering interoperable solutions. Georgia Tech Research Institutes are already doing work in this realm. Through engaging academic institutions use cases could be rapidly developed and tested at relatively low cost. Their research could be published across various public and private sector outlets to disseminate any useful information.

To that end, capitalizing on already available open source solutions and open sourced technologies should be explored. If private vendors are unwilling to be progressive in terms of interoperability furthering publicly available and federally approved EMRs such as OpenEMR should be explored. In terms of interoperable devices there is an abundant code base available on Github for any developer to use and modify to best suit their needs. This includes but is not limited to FHIR resources.

III(B). HAPI on FHIR

The Hapi library already exists for Java with opensource easy to implement step by step instructions for adding FHIR's RESTful Server capabilities to existing applications. Commercial support exists as Smile CDR. The documentation can be found at http://hapifhir.io/doc_rest_server.html#_toc_creating_a_restful_server This is the resource being used by those researching interoperability and working on use cases thus far. This could serve as the FHIR server that the provider's EHR maps to.

In theory a provider could send files over HTTPS, but this leaves the information vulnerable to attack. Using blockchain and a key management system like AWS Key Management System the entire file could be encrypted and held more securely until it is transferred to the requesting provider. It is important to note that the blockchain itself is not transferring the information and the user is not interacting directly with the blockchain. Most of this is handled in the Dapp. The information is still being transferred over using the TCP/IP protocol but the blockchain allows for more robust encryption and audit trails.

III(C). SMART on FHIR

Smart on FHIR functions as the adapter for EMR and apps to work together. An EHR system fills out and stores all the PHI about the patient. That information is in turn stored in the FHIR format. Smart becomes the mechanism to determine what happens before and after access; how 3rd party apps launch within that EMR and what PHI is being accessed. Smart allows for apps to be built on top of it and not have to custom fit integrations into each EMR. It is also important to keep in mind that SMART is a guideline and it falls to the EMR vendor to implement them. Then the health systems must update and configure their systems to encompass these standards.

Once the EMR implementation of SMART was complete it would allow providers to launch their smart on FHIR app within the EMR and either request or sends updates about patients to linked providers both inside and outside of their network.

III(D). Identity management/API access token

The use of tokens allows for a smooth transition between services such between servers inside an outside of a contained system. In our proposed solution a combination of OpenID (which is used to authenticate the user ID to the application without sharing credentials) and Oauth 2.0 (used to grant authorization with only the user ID) and would be ideal. This combination allows for the user to verify their identity and then pass this information off to Oauth 2.0 and grant a token that can be used to request access without passing on the user's identification information specifically. This would allow for a provider to access various servers without having to log in to each one and would allow for traffic without vulnerability.

III(E). Key management system

The Amazon Web Services Key management system allows for simple encryption of sensitive data. Through KMS new public and private keys can be generated and managed for each file. It would require the provider to have a free AWS account. In this proposal AWS would be used to encrypt the patient identifier.

III(F). Blockchain or Distributed Ledgers

The smart contract is key and should be the focus. Users are interacting with the smart contract (or several within the Dapp) to send and receive information. A Dapp can be programmed to execute at given thresholds. For example: if a new file is created within the EMR, a Dapp would automatically send out a request for information from all partners about that particular file, and then populate that information in the EMR without interaction from the provider, or, it could. Be configured to only happen at the click of a button. If a provider decided to refer a patient out, that information could be automatically sent to the next point of care without the provider acting on it. While this is similar to other subscription models available what is novel is the idea of encryption and sharing without an established trust. It would not matter if both providers used the same EMR system if they were both FHIR compliant and used SMART on FHIR integrations to their systems. I would not matter if they even knew the other

provider existed so long as both Provider A and Provider B were both connected to the blockchain. The information would not be flowing from point A to point B, it would be flowing to the blockchain, and would be ready for any one with matching keys to pick up the information and decrypt it. Security is guarantee though the positing of smart contracts in relation to their respective servers. One Dapp between the EHR system and FHIR server, another one between the blockchain and next provider.

It is important in this scenario to keep in mind that the consensus of the underlying blockchain does not matter. That is like asking how packets are cut up and distributed. The user will never interact with the blockchain. It is all done machine to machine. A smart contract can do whatever you program it to do with just the push of a button to changes to a field. Information could be sent out to everyone associated with that provider through subscription. It would be secure thanks to public/private key encryption (just like HTTP/S) and it would not be intrusive to the provider. Currently PHI is sent back and forth across the internet using HTTP/S all the time. This has become common for financial institutions and even medical providers.

III(G). Gaming Theory (Incentives, Positive)

The important focus here is to not become entrenched in the current conversation about ether, gas, etc. These are all tokens used as rewards for gamification and are essentially irrelevant in this context. Providers should share data to guarantee the best care possible to their patients. Rewards of tokens from within the system will not be as incentivizing as outside rewards such as increased funding.

IV. Challenges

IV(A). Cost

There is more hindering interoperability than merely an unwillingness to share data. There is a real cost associated with mapping to FHIR standards. Each EMR can be personalized to suit the needs of the purchaser so a standard method of mapping may not be possible for each system. This would require dedicated time for one or more programmers to not only understand FHIR, but also how to interpret resources and map them appropriately. This effort could not only be time intensive but also labor intensive. For smaller EMR vendors this effort may yield little to no return on investment.

This cost could extend to providers as well. While it would be ideal if integration was handled at the vendor level and pushed as an update to participating EMRs this is unrealistic. Thus, providers may have to hire an outside contractor to configure integration or Healthcare systems may have to divert their IT resources at some cost to them. It is entirely possible, and potentially more plausible to assume that vendors would offer this service to their existing customers at a premium. This is not without precedent, as we have previously discussed this business model is already in use with new features or customization of EMRs.

IV(B). Lack of Incentives/No clear Government Mandates

Without incentives such as reimbursement or funding incentives, the prospect of sharing a potential source of profit does not become of major concern for most vendors or healthcare providers. While having a complete patient history would undoubtedly save time, money and

improve patient care there is still the unwillingness to share data. The fear of penalties for potentially exposing PHI may be enough to deter providers from willingly sharing patient information. The least possible data to be shared is no data.

ARRA was groundbreaking legislation within the United States. Offering positive and negative incentives through the combination of defined expectations in Meaningful Use, manipulation of Medicaid funding, and a clear timeline was a monumental motivator for adoption of Electronic Medical Records systems nationwide. A similar directive beyond the 21st Century Cures act that specified what to use is expected, when, and how (data standards) would spurn adoption.

IV(C). Deviation from standards

In implementing standards such as smart on FHIR healthcare systems and vendors have the options to decided what they do and do not want to implement. This could cause vital information to be lost, even if it has been properly mapped to FHIR. This is where a strong government mandate comes in, if there was a clear, well thought directive in place mandating which resources must be preserved it would allow for more complete data transfers.

IV(D). Scalability

In this scenario the blockchain functions as an index. The block would contain the URL to the FHIR server which housed the patient file. This is due to issues with scalability. "The factors influencing scalability are: bit rate, the frequency of monitoring and transmission, and the amount of information transmitted per patient"[21]. If healthcare records utilized the Bitcoin blockchain, every node on the chain would have a copy of the ledger, which would not only cause issues with latency and block size limits, but also bring questions of security to light[20,12]. Additionally, through-put is limited in the number of transactions and computing power of a node to increase efficiency of transaction processing[15]. The existing infrastructure of blockchain focuses on security and integrity over scalability and plasticity so addressing lag due to volumes of transactions would be difficult[5]. Also, each node would have a copy of every patient record stored on the chain across the country- a concept that is not currently feasible nor secure.

What is possible is to use blockchains that utilize scalable data repositories called data lakes to store records off chain[12]. Data lakes would allow more functionality such as interactive queries, text mining, and machine learning[12]. Data lakes would be maintained and located at point of origin (provider nodes); assuming providers already function on secure networks[22]. All records would be cryptographically signed to guarantee authenticity and file integrity[12].

V. Conclusion

While many functions of healthcare can be streamlined using technology, fragmentation and data transference has not been resolved in the United States. The combination of resistance, lack of mandates and HIPAA guidelines equate to little movement toward interoperability. While blockchain technology could improve interoperability, the technology is still not widely adopted.

Issues of scalability and adherence to HIPAA mean that developing platforms that encourage adoption is tricky. It is evident that within ten years the blockchain technology will evolve to meet

the needs of consumers. Just as the internet evolved rapidly and changed communication, blockchain can grow to meet the needs of healthcare.

The versatility and simplicity in the concept of blockchain make it very attractive. The promise of a transparent ledger seems so simple in concept but in application it becomes difficult. Without government intervention to drive interoperability it will take consumer demand to place pressure on the healthcare establishment to improve information sharing.

It will take time, focus and more use cases to bring blockchain to the forefront of healthcare. Blockchain might be successfully used in healthcare globally before it is able to be used on a large scale in the United States. The very ideas of governance and profitability that have driven the United States to be a superpower may be the biggest hindrance to the adoption and interoperability. Without HIPAA reform and/or improved data security surrounding privacy, governance will continue to stifle potential adoption. Similarly, without the cooperation of vendors at the potential loss of profits, records may never make it to the blockchain to be shared.

Although interoperability is multifaceted and complex understanding some of the human components is imperative. When there are financial incentives to be gained through hoarding data, the likelihood that information blocking will cease organically may be low. Without a strong directive from the government with a mandated EHR and framework for infrastructure, interoperability may be a much longer and more painful process than is necessary.

Additionally, in our research we found little documentation as to the exact financial gain vendors have as a result of locking in customers. Being able to show in dollars and cents how much payers are losing from multiple tests, medication errors, or simply lack of continuity of care could add even more incentive to solve vendor lock in and information blocking.

Our solution requires participation of vendors in the very least to map to FHIR. Outside of mapping very little is needed from vendors, and it falls to providers to adopt and share the information with other providers.

By using open source technology already available the cost of implementation would be relatively low. Because the chain app would be built using SMART on FHIR, integration into the EMR ecosystem should be relatively unobtrusive. The only addition to the provider's work flow on the day to day would be the click of a button. The query, authentication, and encryption or decryption would be handled within the chain apps.

Security is at the forefront of any effort to share information. Through the use of encryption, authentication tokens, unique patient identifiers, and file retention at the point of origin, patient information would be as secure as possible to protect their privacy.

IV. Reference

[1] Adler-Milstein, J., & Pfeifer, E., Information Blocking: Is It Occurring and What Policy Strategies Can Address It?. *Milbank Quarterly*, *95*(1), 117-135, 2017. doi:10.1111/1468-0009.12247

[2] Ahier, B., Three rising technologies that will impact healthcare in 2018. *Health Data Management*.

[3] Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. *Network and Communication Technologies*, *1*(2), 12.

[4] Arndt, R. Z., The long and winding road to patient data interoperability. *Modern Healthcare; Chicago, 47*(18), 2017.

[5] Anjum, A., Sporny, M., & Sill, A., Blockchain standards for compliance and trust. *IEEE Cloud Computing*, *4*(4), 84-90, 2017.

[6] Bender, D., & Sartipi, K. (2013, June). HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. *In IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS)*, 2013 (pp. 326-331). IEEE.

[7] [8] Braunstein, M. L. (2018). Healthcare in the Age of Interoperability: The Promise of Fast Healthcare Interoperability Resources. *IEEE pulse*, 9(6), 24-27.

[8] Heurix, J., Fenz, S., Rella, A., & Neubauer, T. (2016). Recognition and pseudonymisation of medical records for secondary use. *Medical & Biological Engineering & Computing*, *54*(2-3), 371-383. doi:10.1007/s11517-015-1322-7

[9] [33] Hong, J., Morris, P., & Seo, J. (2017, August). Interconnected Personal Health Record Ecosystem Using IoT Cloud Platform and HL7 FHIR. In *IEEE International Conference*

[10] Ivan, D., Moving toward a blockchain-based method for the secure storage of patient records. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*., 2016.

[11] Lapsia, V., Lamb, K., & Yasnoff, W. A., Where should electronic records for patients be stored?. *International journal of medical informatics*, *81*(12), 821-827, 2012.

[12] Linn, L. A., & Koo, M. B., Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.

[13] Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing*, *5*(1), 4.

[14] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K., A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare*, Vol. 1, pp. 1-10, 2016.

[15] Rabah, K., Challenges & Opportunities for Blockchain Powered Healthcare Systems: A Review. *Mara Research Journal of Medicine and Health Sciences, 1*(1), 45-52, 2017.

[16] Reisman, M. (2017). EHRs: the challenge of making electronic data usable and interoperable. *Pharmacy and Therapeutics*, *42*(9), 572.

[17] Walonoski, J., Scanlon, R., Dowling, C., Hyland, M., Ettema, R., & Posnack, S. (2018). Validation and Testing of Fast Healthcare Interoperability Resources Standards Compliance: Data Analysis. *JMIR Medical Informatics*, 6(4).

[18] Winfield, L. (2018). A Look at the Trump Administration's Approach to HIT. *Healthcare Financial Management*.

[19] What Is Hl7 (health Level Seven International)? - Definition from Whatis.com, https://searchhealthit.techtarget.com/definition/Health-Level-7-International-HL7

[20] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G., Metrics for assessing blockchain-based healthcare decentralized apps. In *e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on* (pp. 1-4). IEEE.