Technical Challenges, Ethical Concerns, and Future Opportunities in Interoperable Patient-Centric Medical Data Transfer

Ian Hay, Professor John Rachlin

December 7, 2022

Northeastern University

Boston, MA, 02120

USA

Abstract

The 21st century ushered in the information age and the digitization of many day-to-day tasks and necessities. Governments, including the US', sought to capitalize on this transformation to improve the well-being of their citizens through healthcare. The incentives and mandates proposed by these institutions prioritized adoption and security over a unified and standardized system, leading to fragmented data silos present today. As a result, the transfer of medical data between these systems remains a challenge, and the financial incentives for the companies involved motivates them to retain patient in their network. Additionally, consider the personal and highly sensitive nature of patient's medical information, and the state-of-the-art PDF forms that must be signed to authorize the release of these data. The digitization of electronic health information has enabled more instantaneous and granular access of patient's own medical records, as well as the exchange of these records between systems. Yet such a reality is far from the case in the US to this day. Recent developments and interest in blockchain technology have yielded numerous proof-of-concept networks to exchange medical data between systems, both from the patient level and the healthcare institution level. These technologies lack the ability to transfer the actual data itself, though, and only index the transfer of access control from one party to another. Connecting this access control to health data centers, increasing located on cloud servers, is essential to unlocking the potential of these concepts.

Introduction

The previous two decades of the information age saw the transition from paper to digital health records. The Clinton administration foresaw the change and passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, establishing modern security and privacy guidelines for personal health information [1]. More recently, the Affordable Care Act (ACA), the American Recovery and Reinvestment Act, and the Health Information Technology for Economic and Clinical Health (HITECH) Act passed under the Obama administration in 2009-10 sought to accelerate the transition to electronic health records (EHRs) [2]–[4]. The acts paid out more than $35 billion in subsidies and incentives from 2011 to 2016 to increase EHR adoption across the country [5]. The hope was the digitization of health data would reduce the cost of healthcare and modernize the US' health data systems.

However, the acts were shortsighted in prioritizing EHR adoption and security over a unified, standardized, interoperable system [6]. Hospital systems, keen to cash in on incentives and weary of legal consequences for security flaws, built up proprietary silos to handle EHR data storage and retrieval [7]. The lack of interoperability guidelines meant these data silos largely adopted their own methods for segmenting and aggregating health data. While organizations such as Health Level Seven International curated medical data transaction standards, the complexity of medical data and particularly medical imaging data meant that the storage solutions adopted by hospital systems did not necessarily interoperate with other proprietary systems when transferring data [8]. As a result, in 2014 while more than 80% of office-based physicians had adopted EHRs, 15% of patients had to personally bring a test result to their physician and 5% had to repeat a test due to the unavailability of prior results [9], [10].

To mitigate these issues, new proposals have arisen to prioritize health data interoperability. The non-profit Health Level Seven International group proposed the Fast Healthcare Interoperability Resources (FHIR) standard to exchange resources based on an application programming interface (API) data format standard [11], [12]. The use of API's is particularly important as clinical data has grown tremendously and beginning to be outsourced from local servers to cloud data centers [13]. Recent advancements in blockchain technology could enable a peer-to-peer network of medical data transfer that incentivizes interoperability and data security. Here, we will explore the difficulties associated with medical data transfer, with a particular focus on medical images, opportunities for FHIR API standards and blockchain networks to improve interoperability, and challenges in implementing these technologies while complying with government-mandated privacy standards.

Background

Converting medical data to its digital format is no trivial task. Patient health data represents some of the most complex and sensitive information, and transitioning decades of paper-based records to digital formats is a monumental task. The 1996 HIPAA law mandated that patient medical information is only accessible to the patient and authorized representatives as denoted by the patient themselves [1]. As such, governments around the world sought to incentivize this transition by providing billions of dollars of subsidies with the promise of faster, cheaper, and better health care in the digital age. Ten years after 2009, when the HITECH and American

Recovery and Reinvestment Acts were passed with EHR adoption incentives, EHR adoption doubled [4], [9]. As of writing this paper, 88% of office-based physicians have adopted EHRs. What the governments didn't provide was a standardized system for indexing and segmenting the medical data; this was left to private industry. Eventually, the US government created the United States Core Data for Interoperability (USCDI) in 2016 via the 21st Century Cures Act that mandated the standards medical data and APIs must abide by. The USCDI falls under the US Office of the National Coordinator for Health Information Technology (ONC) and largely draws from commercially created standards and documentation [14]–[16].

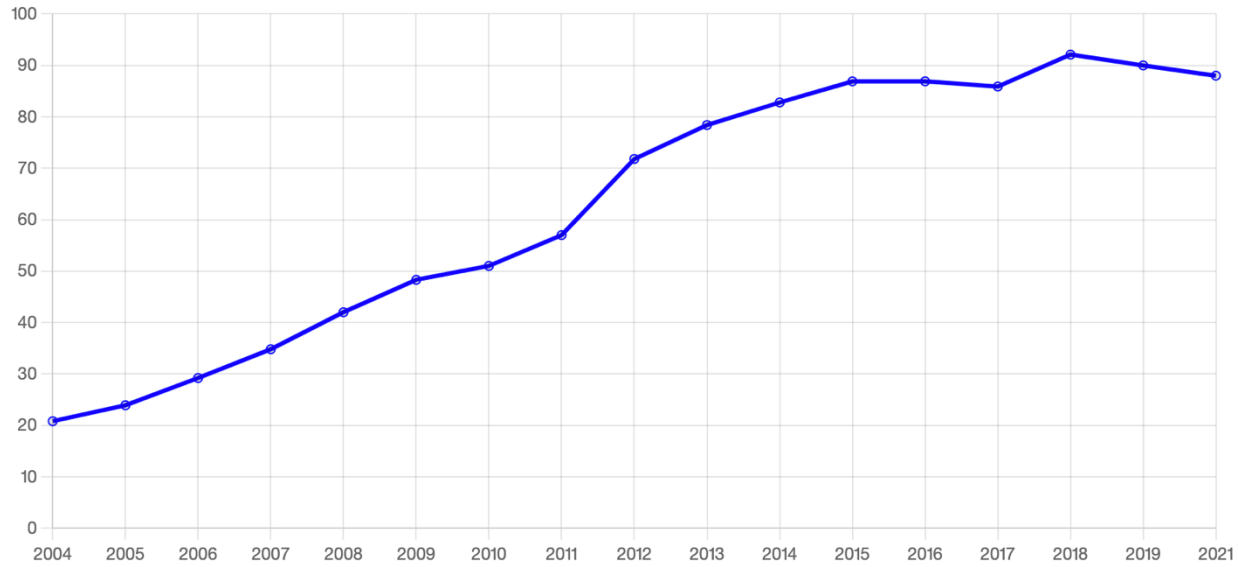

Figure 1: Office-based physician EHR adoption in the US [9].

The Logical Observation Identifies Names and Codes (LOINC) universal medical laboratory data standard was created in 1994 by the non-profit Regenstrief Institute to aid in increasing demand for electronic health databases [17]. It is publicly available with no cost and is cited by the US government in the USCDI documentation. It details the data types and medical terminology to be used in electronic healthcare data. The terminology is split between laboratory and clinical data. For medical images, which comprise a majority of health data by storage size and growth in the 21st century, the Digital Imaging and Communications in Medicine (DICOM) format is most widely used [18]. It details a metadata header with a 2D array of pixels that allows the images to be viewed and important information such as the imaging device and any necessary variables to appear in the header. Notably, DICOM does not store the raw data and the image cannot be re-processed once in DICOM format. For some referrals or consultations where re-rendering the raw image file is necessary, the exchange of DICOM images alone can be a severe downside. Additionally, to comply with HIPAA privacy requirements, the images must either be encrypted or anonymized before sending to cloud server storage, an increasing occurrence as medical data storage and particularly medical images increase in size [13], [19].

The most notable and widely used standard for medical data transfers in clinical settings is Health Level Seven International's version 2 system. The standard defines a messaging system

for exchanging information in a clinical workflow, ranging from patient administration to pharmacy & billing systems. It uses a non-XML syntax based around line segments and character delimiters. The HL7 version 2 standards are desired to be interoperable among all record keeping systems of a hospital workflow and is implemented in every major hospital system in the US [20], [21, p. 7]. Another medical data transfer initiative is Integrating the Health Enterprise (IHE), a non-profit organization created in 1998 to sponsor projects aiming to improve health information sharing. The organization has aided in the US Department of Veterans Affairs health system development and in developing a cross-enterprise document sharing (XDS) model using the LOINC and HL7 standards. They also developed a standard for retrieving medical documents across domains, called the ITI-43 transaction standard [10], [22].

The interoperability of EHRs between vendors and healthcare systems has become a major focus of the ONC in the US. However, as recently as 2019 the transfer of a patient's EHR from one healthcare vendor to another is commonly done via fax or print copies sent via mail. Even for transferring a subset of results for a consultation or referral, the electronic exchange of these documents is only possible roughly 50% of the time, depending on if the different healthcare systems use a vendor with electronic health exchange capabilities between the two systems [8]. To overcome these challenges, the Radiological Society of North America (RSNA) developed the image share network, a clearinghouse-based system where participating healthcare systems send their medical images for sharing to the clearinghouse operator, who stores the images indexed by a cryptographic hash for 30 days. Personal Health Record (PHR) vendors are able to download the patient's information after they authorize it by divulging the token needed to reproduce the hash. While this system eradicates the physical exchange of medical images, it introduces two new, centralized organizations with access to sensitive personal health information. Additionally, early results show that patients are not likely to view or authorize their medical images within the 30-day window, and the image share network is dominated by a small number of radiological centers, and a small number of PHR vendors (who can also act as a clearinghouse operator) control authorized retrieval of medical images [10], [23].

To help mitigate these issues, the Health Level Seven International group proposed the FHIR standard, first drafted in 2011 and officially published in 2017. The standard revolves around APIs to incentive the transfer of data between and within systems; it is built around resources, such as clinical observations, that can be aggregated into FHIR profiles. However, despite endorsements of the standard by the US government, FHIR is still dwarfed in adoption by HL7's version 2 [11].

Technical Challenges

Despite tremendous advancements made in the digitization of health data, the transfer of EHRs between systems remains a challenge to this day. The history of EHR adoption incentives helps understand why. The Medicare Electronic Health Record Incentive Program, which ran from 2011 to 2016 and paid more than $35 billion in subsidies under the Centers for Medicare and Medicaid Services (CMS), set the criteria for physicians and hospital systems to be eligible for EHR adoption bonuses. These criteria include electronic prescription management, active medication and diagnoses lists, vital sign records, and clinical summaries, as well as patient electronic access. Notably, the criteria do not mandate abiding by a particular data or transaction

standard and contain no requirement for interoperability with external systems [6], [24]. With the patient security standards set in the HITECH and HIPAA laws, healthcare data companies were weary of penalties for mismanagement of personal health data and built up proprietary, private silos for storing and retrieving health data.

From the LOINC and HL7 standards came consistent low-level labeling and transfer of medical data; the missing piece is how to group data together to form a database of patient health records or visitation records. The complicated nature of health data and the choices present for EHR vendors to make means clinicians handling EHRs often deal with data fragmentation and missing data [25], [26]. Typically, EHRs are transactional by nature and linked to a single visitation; healthcare providers use registries to link EHR data to a patient's registry [27]. Under the HITECH Act's Meaningful Use mandate, the use of EHRs should operate within the nation's healthcare system in a meaningful manner by allowing patients more direct management of their health data; this is done through the PHR. While EHRs are associated with one or several visits, PHRs are designed to be lifelong records of a patient's medical data [16], [28].

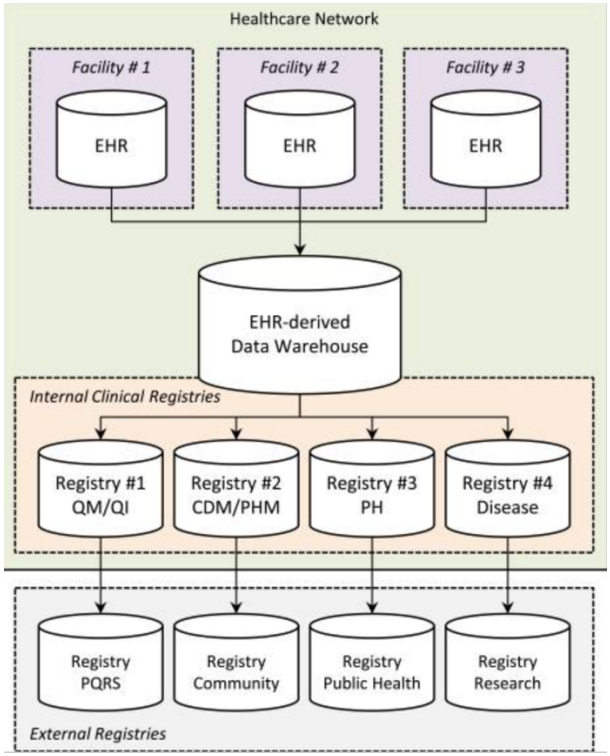

Figure 2: Representative network design of EHR registries for a clinical healthcare provider [16].

The focus shift towards the patient has brought to light issues in aggregating EHRs to form a cohesive and accurate patient health record. Perhaps the most essential data component to link EHRs to the patient's PHR is the patient identifier; these data include the patient's full name, date of birth, home address, and other contact and personal information. The record will also include a unique patient ID record number, and there are commonly three different patient IDs within a hospital system: 1) an internal ID for patient operations, 2) a network-wide ID to

distinguish patients at the healthcare system's numerous facilities, and 3) a regional or statewide ID if the health system is connected to these health information exchanges (HIEs). These patient IDs can then be used to merge EHRs into a registry or PHR [16]. A challenge with this is the registry or PHR provider must locate the patient's master ID through the HIE and reach out to multiple providers to locate the patient's EHRs to aggregate. In many cases, this is not attainable and PHR vendors typically use alternative methods to match patient identifiers, leading to increased mismatches and incomplete or inaccurate data. Match rates, or the rate that a patients EHR is correctly matched to an additional EHR or registry, fall from more than 90% internally to 50-60% outside of a healthcare data system [29].

The transfer of medical images presents its own unique challenges, and overcoming these barriers is essential to creating interoperable health data systems. The average healthcare provider manages more than 600 terabytes of patient information, with up to 80% of that data by storage size being unstructured medical images [30]. Moreover, medical images represent up to 90% of medical data growth, forecast to reach 2.3 zettabytes in 2022 [31]. Images are commonly stored as either the raw or proprietary file formats output from the medical imaging device, or as rendered images of a standardized format (typically DICOM). Currently, challenges exist for healthcare systems that maintain both raw and rendered DICOM images in linking files together from the same study [19]. Additionally, it can be difficult to maintain the data viability of proprietary data formats, which can be necessary to elucidate insights for a radiologist examining the image [18]. With medical data increasing exponentially in size, health data systems are moving medical data to offsite cloud computing storage, the images must either be encrypted or anonymized to comply with HIPAA. This presents a challenge in storing raw images, as they must be de-encrypted on-site to render the image, removing much of the benefit of cloud computing power. Anonymized images are also a possibility, particularly for sharing images or data with a broader audience (for example, in creating a public medical imaging dataset for machine learning). However, linking these images back to their patient presents a challenge for clinical use, and anonymization techniques have proven at times ineffective at truly removing personal identifiable information [19].

Despite advancements in the storage and standardization of medical images, transferring these objects outside of a health data system remains a challenge. The image sharing network proposed by the RSNA has attracted few participants, and as such the physical transfer of medical images via CDs or DVDs remains viable to this day [10]. The technical challenges are largely associated with ensuring accurate patient identification between systems and correctly linking raw and DICOM-formatted medical images together with their patient or study in both the sending and receiving platforms.

Patient Privacy Considerations

Notably, the technical challenges associated with medical data sharing between systems are not infeasible to solve. The issue in promoting interoperability comes from the growth of these data systems themselves and the financial incentive to upkeep the status quo. Governments, including the US government, poured tens of billions of dollars to incentivize EHR adoption with minimal interoperability requirements. Now, with large EHR data silos already in place, there are no requirements, mandates, or subsidies to convert these platforms to interoperable standards,

including HL7's FHIR standard (as of July 2021, the CMS does require availability of patient records in the FHIR standard, but only for Medicare and Medicaid patients, compromising around 135 million individuals or roughly 40% of the American population [32]–[34]). Additionally, consider that these health data systems only make money on the patients and hospitals that continue to use their platform; they are incentivized to minimize interoperability and keep customers on their service. Hospital systems are satisfied with this; so long as the data service is adequate at providing internal health data management, it can ensure that existing patients remain with the hospital system. This lack of interoperability harms the patients, as they do not have easy access to the best care available if that care is outside of their existing care provider's system. Thus, the parties with the onus to promote interoperability in their health data systems are simultaneously incentivized to maintain the "walled garden" standard we have grown accustomed to, while the patients with minimal say in the matter are most negatively impacted.

Patient considerations don't stop there, though. When a patient is admitted to a hospital or care provider for the first time, they are asked to sign a release form for their personal health information. HIPAA mandates the patient be made aware of their privacy rights: what information will be shared, for what purpose, and with whom; once signed, the healthcare provider does not need to ask for consent or authorization again [35]. The healthcare provider may also ask patients to allow electronic health information exchange by granting access permission to EHR vendors and service providers [36]. Additionally, hospitals do not need patient consent to transfer or even sell de-identified personal health information, resulting in the founding of Truveta, a company selling near real-time clinical data on over 50 million patients in the US aggregated from 14 healthcare systems [37].

With health data moving to primarily digital storage and retrieval, giving patients granular access controls of their data is more possible than ever. With patient's personal health data being sensitive and innately personal, this must be considered to maintain patient's trust and consideration in the healthcare system. Patients with rapid electronic control over their data may be more likely to share clinically applicable data with relevant research studies without requiring the data to be de-identified, giving the researchers more variables to consider. However, there are key cybersecurity concerns with giving each patient access control over their own data. Data breaches have stolen more than 100 million patient's records through existing secure storage mechanisms; granting patients access controls could open them to additional phishing scams already prevalent in financial accounts [38]. It is worth noting that the current state of the art, based on these figures, is far from perfect and the personal data considerations of giving patients control of their data may outweigh the feasible increase in phishing attacks. This warrants at least investigating the benefits and drawbacks of patient control. Such a solution must nonetheless try to minimize the potential for these phishing scams.

Blockchain-based Solutions

One growing technology that has begun to take attention from EHR engineers is blockchain. A peer-to-peer network with native cryptographic security presents a promising avenue to exchange health data between institutions. Indeed, several initiatives have presented different proof-of-concept approaches to developing blockchain-based EHR exchanges, each of which

will be explored later in this section. First, it's important to understand where blockchain can provide solutions, and where it cannot, in the secure transfer of personal medical data.

A blockchain, broadly, is a linked list (or chain) of blocks containing transaction data. These messages, or transactions, can theoretically transfer any digital asset, from cryptocurrencies to pieces of data, moving from the sender to the receiver identified by their public cryptographic keys. The sender will sign their transaction with their private key, and the receiver can verify the sender signed the message before the transaction is broadcast to the network. The blockchain network will then include the verified transaction in an upcoming block's message, where it will be integrated in the blockchain permanently. There are two underlying blockchain architectures that can be selected for network design: permission and permissionless. In a permissionless blockchain, all nodes are created equal, and any node can post or verify transactions on the network, with a certain cost associated. These networks are commonly used to form trustless financial networks, with the most notable being Bitcoin and Ethereum. Permissioned blockchains, on the other hand, have various levels of permissions associated with each node, granting a form of access control over who can and how to interact with the network. These are used to form trusted, private networks, most notably using the Hyperledger Fabric architecture publicly available from the Linux Foundation. Once a block has been published to the network, it cannot be changed outside of a malicious attack. Hence, blockchains are commonly thought of as an append-only database across a distributed network. More detailed reviews of the various forms of blockchains and the math behind their cybersecurity are widely available and outside the scope of this manuscript [39]–[43].

A peer-to-peer blockchain network presents some beneficial attributes for inter-system health data exchange. First, the native cryptographic security of blockchain messages prevents malicious actors from directly intercepting transactions. The peer-to-peer nature of the network also removes the need for a clearinghouse, which poses as a single point-of-failure for attacks, such as social engineering. Since transactions are broadcast to the entire network, malicious transactions can be flagged and voided: for instance, if a hospital attempts to send millions of records to a single wallet with no prior transactions and no publicized rationale, the network can choose to not include that transaction in their upcoming blocks [44]. More recent advancements in cryptographic technology have enabled access control and revocation of permission via proxy re-encryption (PRE) [45]. Finally, creating a network of health systems can standardize transactions (for example, mandate using HL7's FHIR to broadcast transactions) and patient identifiers via their public key, a notable issue with inter-system data exchange today as mentioned above.

However, a blockchain-based transaction system will not magically solve all the issues with EHR data transfer between systems. First, cryptographic networks like blockchains are still susceptible to phishing attacks; if a user's private key is compromised, their data is at risk. Importantly, a blockchain also only guarantees the cryptographic security of data stored on the network's blocks. With the growth and complexity of medical data, storing the data itself on chain is computationally infeasible; thus, the blockchain would instead only include the transaction messages and not the actual data in these implementations [10]. Additionally, as an append-only and immutable database, the data lifecycle becomes another issue [30]. Standardizing the lifecycle of clinical data between healthcare systems may prove challenging

and controlling the lifecycle of file types for proprietary raw medical images, for instance, may be impossible with hospitals using different medical devices and associated software tools.

Finally, it is important to consider whether a blockchain is necessary to provide the solutions needed for interoperable medical data exchange. As hospital systems desperately need to improve transfer between systems, establishing a peer-to-peer network of cryptographically secure transactions through a distributed ledger is a promising solution to handling the transaction standards of data exchange. State entities with large stakes in the matter, such as national governments, can also provide incentives through blockchain network rewards to increase adoption and investment into the system, and mandate that patient's medical data be made transferrable through the network to create a truly interoperable system of health data exchange [10]. Patients could even be granted more granular access control of their own data through their private key, enabling rapid sharing of medical data with known parties when necessary and giving patients increased control of their personal information [46]. However, the issue of securely transferring the data itself is another important challenge that blockchain alone cannot solve. Establishing more advanced cryptographic techniques to allow access control of cloud-stored medical data integrated through blockchain transactions without relying on the cloud provider to maintain a list of private encryption keys may be. This is an active area of research for cryptography and could enable blockchain-based solutions to take shape [47]–[49].

There are several ongoing blockchain-based initiatives for EHR medical data exchange. The two architectures explored below endure antagonistic approaches to accomplish their mission.

The first initiative to explore is HealthChain, a permissioned blockchain built around patient-controlled access and interoperability. It is designed around HL7's FHIR standard for medical data transfers via API, meaning participants must use this standard to publish transactions on the blockchain. Additionally, it uses PRE to revoke access to medical records, which is necessary to amend or update patient records or correct for incorrectly linked patient records. To accomplish all of this, it uses a mixed-block approach to the network where every other block is of the same type. The first flavor of block is the patient block, a revokable, permissioned index of patient's access control transactions over their own personal medical data. Patients are permissioned nodes capable of controlling access over their own data through their private key and PRE and are the only ones capable of committing transactions to patient blocks. The other block type is a log block, a permissionless, immutable record of all transactions. It is used to audit the system and provides a history of every transaction within the network. This project is available as an open codebase linked with the original paper [46].

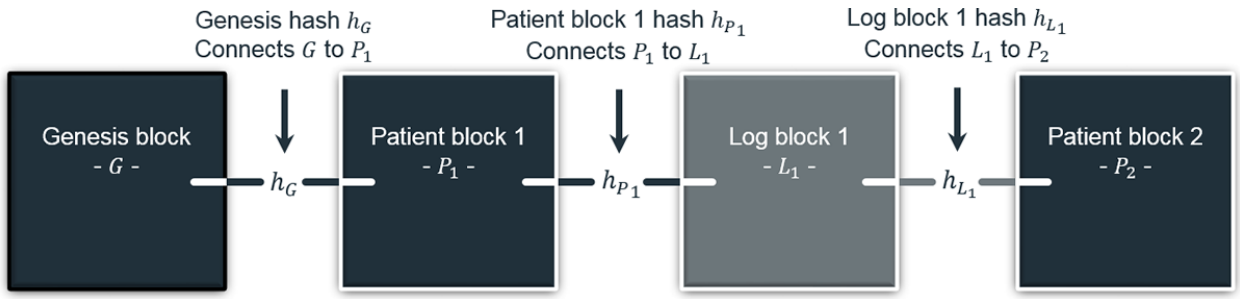

Figure 3: HealthChain's mixed-block architecture [46].

A different approach to medical imaging data exchange is presented in MIFS, or Medical Image File Sharing. This architecture is built towards medical image exchange and with health system-level access control with the goal of increasing the availability of clinical data for machine learning research. Each hospital system would operate their own node, called a FileNode, to handle their respective clinical imaging data. The metadata of images would be stored in the hospital's FileNode, which the images themselves would be stored externally to reduce the blockchain's resource burden. Organizations would enter the permissioned blockchain via a certificate authority and a membership identity provider. Users of the hospital system could then upload images, which would be encrypted to comply with HIPAA, encoded into slices and stored in the FileNode. The proof-of-concept system was built by the authors through Hyperledger Fabric and a RESTful Java API, and is detailed in their paper [7].

Discussion

Despite advancements in EHR software and updated data standards, inter-system transfer of patient medical data remains a challenge to this day. There are several technical and ethical issues for this. From a technological standing, it is difficult to aggregate and identify patient records between fragmented hospital systems, and without a national registrar of patient identifiers these EHR vendors rely of personal information to identify individuals. Additionally, data storage growth for medical images has made locally storing medical data on a hospital scale nearly impossible, leading to the outsourcing of these data to cloud computing providers. While this has solved the data storage issue, it has created new challenges in the form of verifying identity and access control of medical data. To send personal medical data to the cloud it must be encrypted to protect the patient's privacy and must be decrypted to return to a workable state for clinical use. Transferring the encrypted images to another party is redundant without providing a manner for decrypting that data but giving the cloud provider the means to decrypt the data (in the form of its private key) is a major security risk.

Major hurdles exist in the ethical issues of medical image interoperability. Hospital systems and EHR vendors would be negatively impacted by adjustments that make it easier for patients to leave their system for a competitor. Additionally, companies make millions of dollars farming tens of millions of patient health records to sell to health data companies. Providing patients with increased access control over their own data would dwindle these opportunities. As such, the move to interoperable health systems is unlikely to happen without massive incentive or mandates, as was the case when the goal was to promote EHR adoption as a means of improving and modernizing patient's healthcare.

Blockchain technology has made many headlines in recent years for its speculative investment bubbles and potential to digitize finance beyond existing capabilities. With the large spike in interest and the subsequent minimal impact in day-to-day lives, many have begun to question where it might be beneficial to have a peer-to-peer, append-only distributed ledger. The transfer of medical images between hospital systems may be an opportune use case. Cyberattacks consistently target medical data as some of the most personal and sensitive information available to exploit individuals and maintaining this data security in transfer between siloed systems is essential to maintaining patient privacy. Establishing cryptographically secure connections

between these systems, with public keys identifying each participant and a distributed ledger showcasing all transactions, promises to be a method for interoperable transfer of sensitive personal health information. However, these networks are notoriously computationally expensive, and cannot conceivably store the transferred data for all medical patients in the US. Thus, solutions posed for medical data transfer with blockchain technology only publish the transactions between parties on the network, with the data in transfer and stored externally. Key to making these solutions viable is connecting the network's transactions to cloud computing providers who will inevitably store an increasing proportion of all medical data. Zero-knowledge proofs offer a potential solution for allowing data owners to prove access control over their data without revealing their private key or the underlying data to any party.

Conclusion

The road to EHR adoption in the US has been paved by massive government incentives for nationwide adoption. Those resources have since dried up as adoption plateaued in the mid-2010's, and while more than 90% healthcare providers have some form of electronic health data management, the interexchange of these data between systems has proven a challenge to this day. Initiatives pioneered by groups such as HL7 and IHE implore health data systems to adopt interoperability have garnered support from government agencies, but adoption of these standards has been slow compared to existing systems. This can be attributed to numerous factors: the lack of government incentives to adopt these standards, and the negative financial incentives to promote users fleeing their current health system. As health data has been digitized, the patient release of personal health information has remained a static written form with minimal granularity and control to the patient over their own health data. Advancements and renowned interest in blockchain technology has opened the possibility for this cryptographic ledger to serve as a platform for health information exchange between systems. Several initiatives have begun to explore architectures for these platforms with different focuses in the product. As the technology grows, important advancement in cryptographic techniques to connect these blockchain-based access control to cloud computing permissions is essential to creating a real-world system. Development in this space, along with incentives from large actors like governments, may be the solution to solving the interoperability issue plaguing medical data exchange in the US today.

References

[1] P. F. Edemekong, P. Annamaraju, and M. J. Haydel, "Health Insurance Portability and Accountability Act," in *StatPearls*, Treasure Island (FL): StatPearls Publishing, 2022. Accessed: Nov. 06, 2022. [Online]. Available: http://www.ncbi.nlm.nih.gov/books/NBK500019/

[2] S. F. Fontenot, "The Affordable Care Act and electronic health care records: can technology help reduce the cost of health care?," *Physician Exec.*, vol. 40, no. 1, pp. 68–72, Feb. 2014.

[3] S. Freymann Fontenot, "The Affordable Care Act and electronic health care records. Does today's technology support the vision of a paperless health care system?," *Physician Exec.*, vol. 39, no. 6, pp. 72–74, 76, Dec. 2013.

[4] M. Butler, "Top HITECH-HIPPA compliance obstacles emerge," *J. AHIMA*, vol. 85, no. 4, pp. 20–24; quiz 25, Apr. 2014.

[5] "CMS EHR Incentive Program - November 2016 Report," p. 5, 2012.

[6] A. Wright, J. Feblowitz, L. Samal, A. B. McCoy, and D. F. Sittig, "The Medicare Electronic Health Record Incentive Program: Provider Performance on Core and Menu Measures," *Health Serv. Res.*, vol. 49, no. 1 Pt 2, pp. 325–346, Feb. 2014, doi: 10.1111/1475-6773.12134.

[7] H. Liu, X. Xiao, X. Zhang, K. Li, and S. Peng, "MIFS: A Peer-to-Peer Medical Images Storage and Sharing System Based on Consortium Blockchain," in *Bioinformatics Research and Applications*, Cham, 2021, pp. 336–347. doi: 10.1007/978-3-030-91415-8_29.

[8] T. H. Payne *et al.*, "Status of health information exchange: a comparison of six countries," *J. Glob. Health*, vol. 9, no. 2, p. 020427, doi: 10.7189/jogh.09.020427.

[9] "Office-based Physician Electronic Health Record Adoption | HealthIT.gov." https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption (accessed Nov. 07, 2022).

[10] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics J.*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[11] M. Ayaz, M. F. Pasha, M. Y. Alzahrani, R. Budiarto, and D. Stiawan, "The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities," *JMIR Med. Inform.*, vol. 9, no. 7, Art. no. 7, Jul. 2021, doi: 10.2196/21929.

[12] E. R. Pfaff *et al.*, "Fast Healthcare Interoperability Resources (FHIR) as a Meta Model to Integrate Common Data Models: Development of a Tool and Quantitative Validation Study," *JMIR Med. Inform.*, vol. 7, no. 4, Art. no. 4, Oct. 2019, doi: 10.2196/15199.

[13] Y. Duan, Y. Li, L. Lu, and Y. Ding, "A faster outsourced medical image retrieval scheme with privacy preservation," *J. Syst. Archit.*, vol. 122, p. 102356, Jan. 2022, doi: 10.1016/j.sysarc.2021.102356.

[14] S. K. Magid, K. Cohen, and L. S. Katzovitz, "21st Century Cures Act, an Information Technology-Led Organizational Initiative," *HSS J.*, vol. 18, no. 1, pp. 42–47, Feb. 2022, doi: 10.1177/15563316211041613.

[15] "United States Core Data for Interoperability (USCDI)." https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi (accessed Nov. 07, 2022).
[16] V. Ehrenstein, H. Kharrazi, H. Lehmann, and C. O. Taylor, *Obtaining Data From Electronic Health Records*. Agency for Healthcare Research and Quality (US), 2019. Accessed: Nov. 14, 2022. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK551878/
[17] C. J. McDonald *et al.*, "LOINC, a Universal Standard for Identifying Laboratory Observations: A 5-Year Update," *Clin. Chem.*, vol. 49, no. 4, pp. 624–633, Apr. 2003, doi: 10.1373/49.4.624.
[18] M. Larobina and L. Murino, "Medical Image File Formats," *J. Digit. Imaging*, vol. 27, no. 2, pp. 200–206, Apr. 2014, doi: 10.1007/s10278-013-9657-9.
[19] S. G. Langer, "Challenges for Data Storage in Medical Imaging Research," *J. Digit. Imaging*, vol. 24, no. 2, p. 203, Apr. 2011, doi: 10.1007/s10278-010-9311-8.
[20] "Standards Organizations for the NHII," *ASPE*. https://aspe.hhs.gov/standards-organizations-nhii (accessed Nov. 07, 2022).
[21] "Introduction to HL7 Standards | HL7 International." http://www.hl7.org/implement/standards/index.cfm?ref=nav (accessed Nov. 07, 2022).
[22] D. A. Clunie, D. K. Dennison, D. Cram, K. R. Persons, M. D. Bronkalla, and H. "Rik" Primo, "Technical Challenges of Enterprise Imaging: HIMSS-SIIM Collaborative White Paper," *J. Digit. Imaging*, vol. 29, no. 5, pp. 583–614, Oct. 2016, doi: 10.1007/s10278-016-9899-4.
[23] S. G. Langer *et al.*, "The RSNA Image Sharing Network," *J. Digit. Imaging*, vol. 28, no. 1, pp. 53–61, Feb. 2015, doi: 10.1007/s10278-014-9714-z.
[24] "Medicare & Medicaid EHR Incentive Program Registration & Attestation System." Centers for Medicare and Medicaid Services, 2013a. [Online]. Available: https://ehrincentives.cms.gov/hitech/login.action
[25] M. Quinn *et al.*, "Electronic Health Records, Communication, and Data Sharing: Cchallenges and Opportunities for improving the diagnostic process," *Diagn. Berl. Ger.*, vol. 6, no. 3, pp. 241–248, Aug. 2019, doi: 10.1515/dx-2018-0036.
[26] B. J. Wells, K. M. Chagin, A. S. Nowacki, and M. W. Kattan, "Strategies for Handling Missing Data in Electronic Health Record Derived Data," *eGEMs*, vol. 1, no. 3, 2013, doi: 10.13063/2327-9214.1035.
[27] C. A. Caligtan and P. C. Dykes, "Electronic Health Records and Personal Health Records," *Semin. Oncol. Nurs.*, vol. 27, no. 3, pp. 218–228, Aug. 2011, doi: 10.1016/j.soncn.2011.04.007.
[28] M. Lester, S. Boateng, J. Studeny, and A. Coustasse, "Personal Health Records: Beneficial or Burdensome for Patients and Healthcare Providers?," *Perspect. Health Inf. Manag.*, vol. 13, no. Spring, p. 1h, Apr. 2016.
[29] G. Morris *et al.*, "Patient Identification and Matching Final Report," p. 93, 2014.
[30] H. Jin, Y. Luo, P. Li, and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/ACCESS.2019.2916503.
[31] "Cloud migration for medical imaging data using Azure Health Data Services and IMS." https://azure.microsoft.com/en-us/blog/cloud-migration-for-medical-imaging-data-using-azure-health-data-services-and-ims/ (accessed Nov. 21, 2022).

[32] "CMS Interoperability and Patient Access final rule | Guidance Portal." https://www.hhs.gov/guidance/document/cms-interoperability-and-patient-access-final-rule-0#CMS-Interoperability-and-Patient-Access-Final-Rule (accessed Nov. 28, 2022).
[33] "CMS Releases Latest Enrollment Figures for Medicare, Medicaid, and Children's Health Insurance Program (CHIP) | CMS." https://www.cms.gov/newsroom/news-alert/cms-releases-latest-enrollment-figures-medicare-medicaid-and-childrens-health-insurance-program-chip#_ftn1 (accessed Nov. 28, 2022).
[34] "NA_EST2021_POP: Monthly Population ... - Census Bureau Table." https://data.census.gov/table?tid=PEPNATMONTHLY2021.NA_EST2021_POP&hidePreview=false (accessed Nov. 28, 2022).
[35] R. A. Tariq and P. B. Hackert, "Patient Confidentiality," in *StatPearls*, Treasure Island (FL): StatPearls Publishing, 2022. Accessed: Nov. 26, 2022. [Online]. Available: http://www.ncbi.nlm.nih.gov/books/NBK519540/
[36] "Health Information Privacy Law and Policy | HealthIT.gov." https://www.healthit.gov/topic/health-information-privacy-law-and-policy (accessed Nov. 27, 2022).
[37] "Our Approach to Data Quality." Truveta, Spring 2022. Accessed: Nov. 27, 2022. [Online]. Available: https://www.truveta.com/wp-content/uploads/2022/06/whitepaper-data-quality.pdf
[38] K. P. Seastedt *et al.*, "Global healthcare fairness: We should be sharing more, not less, data," *PLOS Digit. Health*, vol. 1, no. 10, p. e0000102, Oct. 2022, doi: 10.1371/journal.pdig.0000102.
[39] N. K. Tran and M. A. Babar, "Anatomy, Concept, and Design Space of Blockchain Networks," in *2020 IEEE International Conference on Software Architecture (ICSA)*, Mar. 2020, pp. 125–134. doi: 10.1109/ICSA47634.2020.00020.
[40] L. Lesavre, P. Varin, and D. Yaga, "Blockchain Networks: Token Design and Management Overview," National Institute of Standards and Technology, Feb. 2021. doi: 10.6028/NIST.IR.8301.
[41] V. G. Martínez, L. Hernández-Álvarez, and L. H. Encinas, "Analysis of the Cryptographic Tools for Blockchain and Bitcoin," *Mathematics*, vol. 8, no. 1, Art. no. 1, Jan. 2020, doi: 10.3390/math8010131.
[42] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," *Financ. Innov.*, vol. 5, no. 1, p. 27, Jul. 2019, doi: 10.1186/s40854-019-0147-z.
[43] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 9.
[44] V. Kanth, J. McEachen, and M. Tummala, "Parameter Identification for Malicious Transaction Detection in Blockchain Protocols," in *Blockchain and Applications*, Cham, 2022, pp. 54–63. doi: 10.1007/978-3-030-86162-9_6.
[45] X. Xu, X. Dong, X. Li, G. He, and S. Xu, "Patient-Friendly Medical Data Security Sharing Scheme Based on Blockchain and Proxy Re-encryption," in *Web Information Systems and Applications*, Cham, 2022, pp. 615–626. doi: 10.1007/978-3-031-20309-1_54.
[46] R. H. Hylock and X. Zeng, "A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study," *J. Med. Internet Res.*, vol. 21, no. 8, p. e13592, Aug. 2019, doi: 10.2196/13592.
[47] F. Zhang, X. Fan, P. Zhou, and W. Zhou, "Zero knowledge proofs for cloud storage integrity checking." arXiv, Dec. 01, 2019. doi: 10.48550/arXiv.1912.00446.

[48] V. Agarwal, A. K. Kaushal, and L. Chouhan, “A Survey on Cloud Computing Security Issues and Cryptographic Techniques,” in *Social Networking and Computational Intelligence*, Singapore, 2020, pp. 119–134. doi: 10.1007/978-981-15-2071-6_10.
[49] H. Liu and D. Han, “Non-interactive Zero Knowledge Proof Based Access Control in Information-Centric Internet of Things,” in *Algorithms and Architectures for Parallel Processing*, Cham, 2022, pp. 617–631. doi: 10.1007/978-3-030-95388-1_41.