BLOCKCHAIN™ IN HEALTHCARE TODAY

# OpenPharma Blockchain on FHIR: An Interoperable Solution for Read-Only Health Records Exchange through Blockchain and Biometrics

Gracie Carter,[1] Benjamin Chevellereau,[2] Hossain Shahriar,[1] Sweta Sneha[1]

**Affiliations:** [1]Kennesaw State University, Kennesaw, Georgia; [2]Certara, Princeton, New Jersey

**Corresponding Author**: Dr. Sweta Sneha, Kennesaw State University, 560 Parliament Garden Way NW, Room 491, Kennesaw, GA 30144. ssneha@kennesaw.edu

**Keywords:** Biometric, Blockchain, Electronic Medical Records, EMR, Fast Health Interoperable Resource FHIR, Healthcare, Interoperability, OpenPharma

**Section:** Methodologies/API

*The healthcare system in the United States is unique. From payor to provider, patients have the freedom of choice. This creates a complicated and profitable paradigm of care. Legislation defines government expectations of data exchange; however, the methods are left to the discretion of the stakeholders. Today, devices and programs are not built to unified standards, thus they do not share data easily. This communication between software is known as interoperability. We address the health data interoperability by leveraging Fast Health Interoperable Resource (FHIR) standard, a viewer of FHIR called OpenPharma, and Blockchain technology. Our proof of concept, called "OpenPharma Blockchain on FHIR" (OBF), is interoperable by design and grants clinicians access to patient records using a combination of data standards, distributed applications, patient-driven identity management, and the Ethereum blockchain. OBF is a trustless, secure, decentralized, and vendor-independent method for information exchange. It is easy to implement and places the control of records with the patients.*

Since 2009, new technologies, such as distributed ledgers (blockchains) and Electronic Medical Records (EMR), have introduced new possibilities for information exchange. The Health Information Technology for Economic and Clinical Health (HITECH) Act passed in 2009 pushed healthcare in the United States into the digital age. HITECH, set aside nearly $27 billion (€24 billion) over the course of 10 years[1,2] in incentives and emphasized EMRs for improved care quality, efficiency, and error prevention. HITECH introduced incentives among providers to digitize medical records and adopt EMR systems.[1–3]

The intention of legislation was to improve information exchanges between providers.[4] HITECH mandated creation of an infrastructure for a nationwide health information exchange that allowed for the flow of health information electronically[5] but included no systems or standards for data sharing. EMRs streamlined records, but records and data still remain contained in the originating health system.[5] Record transmittal to the next point of care is not guaranteed because of the inability or unwillingness to share complete records.[6] Common hindrances cited as reasons for noninteroperability, such as vendor lock in, security, lack of data integrity, and system incompatibilities, can be overcome using OpenPharma Blockchain on FHIR (OBF).

System-level incompatibilities are referred to as vendor lock-in. While locked in, providers cannot migrate to another vendor without compromising revenue and/or information integrity. The most common forms of vendor lock-in for EMRs are proprietary ownership, refusal to modify, competition between different vendors on the market, or cost-prohibitive fees associated with modifications.[7] With these barriers, there is no guarantee that data can be transferred from one EMR system to another while maintaining file integrity.[7]

Upon purchase from a vendor, customers are offered incentives for vendor loyalty in future purchases. To ensure dependency, proprietary software may render data incompatible with third-party software.[7] Among providers, 49% of those surveyed stated that EMRs routinely block information by intentionally limiting interoperability, charging high fees for exchanges, and making Act is difficult or impossible.[8] This method of lock-in originates and is controlled by the vendors themselves. It is highly effective because it makes data migration an arduous or impossible.[9]

Vendors often require that they be the sole source of support for the software. If customers want part of their system modified, that may require an additional purchase from the vendor. More revenue can be gained through guarding information and charging systems to modify it.[9]

With innovation, competition among vendors increases. If a vendor is able to innovate, it becomes a powerful marketing tool. The ability for vendors to market their products in this manner attracts customers to new functions but may overshadow less functional features, which may be better with another system. Additional components and features also allow for differing price tiers. However, new features[10] may add information exchange complications between systems without adherence to a common data standard. Having access to add-ons or plug-ins developed by trusted third parties would allow greater access to desired functionalities without purchasing a new system.

As the 21st Century Act is enabling development of new medical devices and tools faster, there is a tremendous need to be able to share data within devices and with EHR systems.

**DATA STANDARDS**

Using a common data standard allows systems to exchange information seamlessly. Once transmitted to another point of care, the information could be directed to the appropriate field in the recipient's system through information mapping. The obstacle is not that a standard does not exist, or the inability to implement. Rather, it is the lack of willingness to commit resources to share data by EMR vendors.

Recognizing the noninteroperability issue, the Centers for Medicaid & Medicare Services

(CMS) released a request for information for possible solutions for interoperability in 2019.[11] Where CMS funding goes, healthcare follows. In 2019, CMS officially endorsed adherence to Fast Health Interoperable Resource (FHIR) standards those who did not or could not risk losing.[11]

**Technology Used**

Figure 1 provides an overview of OBF for an example patient, John Doe, who provides data in Hospital A, and eventually the same data gets shared, secured to Specialist S through voice authentication, storing of encrypted URL data within blockchain.

Because our proposed OBF is a proposed architecture, adding a security layer can be achieved with an available blockchain technology such as Ethereum and Hyperledger. The Ethereum blockchain was chosen for maturity. Other choices are possible for the blockchain such as Hyperledger. The current discourse in healthcare interoperability is

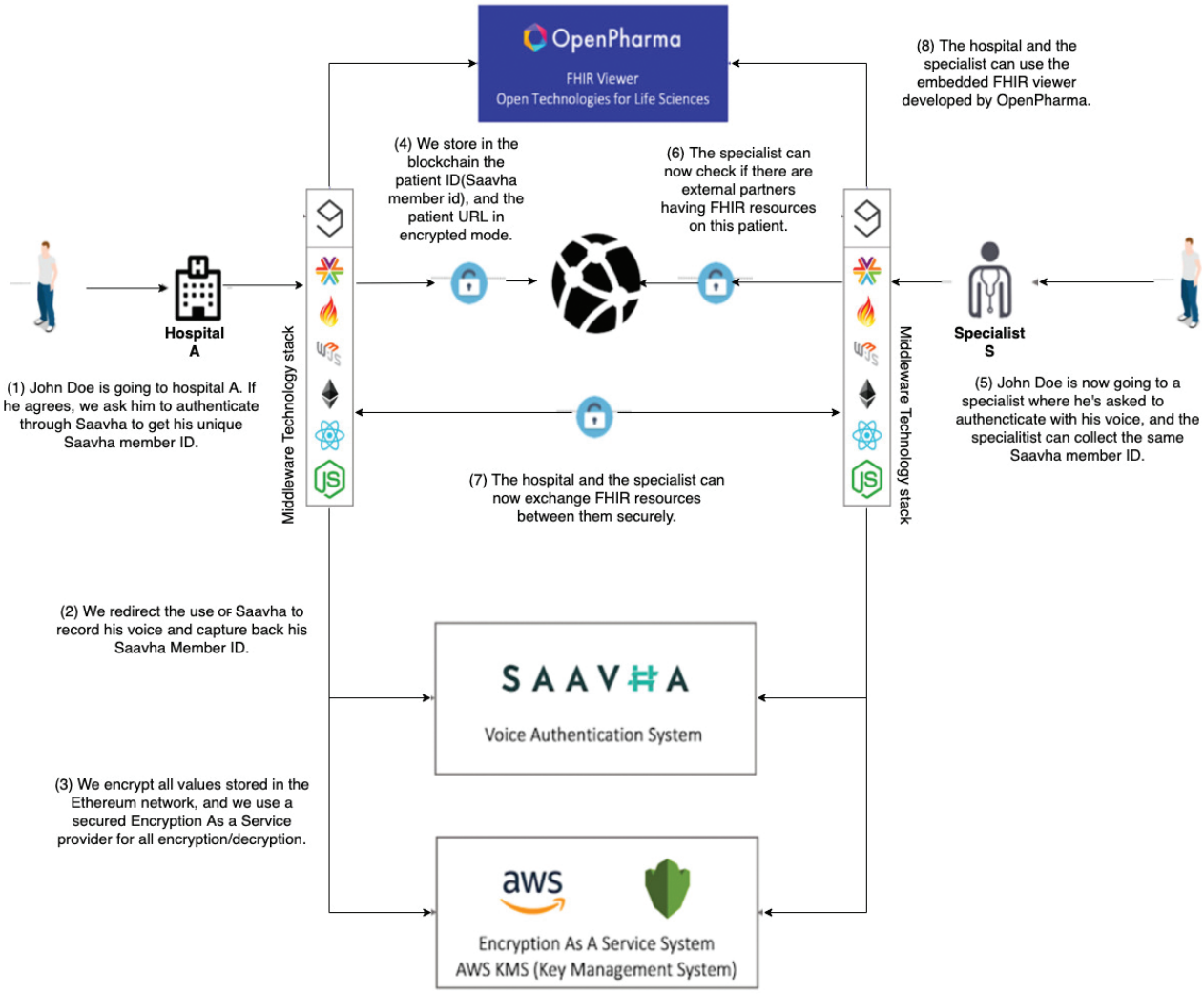


*Figure 1—An overview of OpenPharma Blockchain on Fast Health Interoperable Resource. AWS: Amazon Web Services.*

centered on data ownership and transparency; we believe that a private permissioned blockchain is counter to ownership. A privately held blockchain is simply a data silo. It is only through complete transparency that data are secure. Without a centralized authority and through the decentralization of data across a blockchain, fear of data hoarding or abuse are assuaged. Users can be rest assured that data are accurate and safe[12] through audit trails of access authorization.[2] For the first time, data owners (the patients) are completely aware of who has access to their records and hold providers accountable for alteration of records.[13] Because a blockchain can update in near real time, the data would always be current and accessible if authorized.[14,15]

All Ethereum transactions use Solidity coding scripts to execute specified functions automatically, known as smart contracts.[16] A smart contract is executed based on a predefined trigger without human action or oversight, adding to reliability and security.[16]

SAAVHA is a voice authentication system. It accepts user voice and returns a unique signature, which can be used as an ID, independent of PHI.

## PROPOSED OBF FRAMEWORK

Figure 2 presents the overview of the Framework of OBF and further details about encryption and the process flow. The OBF application includes the following for middleware: SMART on FHIR to launch the app in the EMR, FHIR resources for semantic interoperability between providers, the Smart Contract to store members' IDs, partner ping URLs and patient resource URLs, information web3.js to interact with Ethereum, React for frontend and implemented in node.js. Outside applications include Ethereum blockchain to store and make encrypted data available to partners, SAAVHA for biometric validation, Amazon Key Management Service (KMS) for encryption, and OpenPharma FHIR viewer to view patient files without downloading.

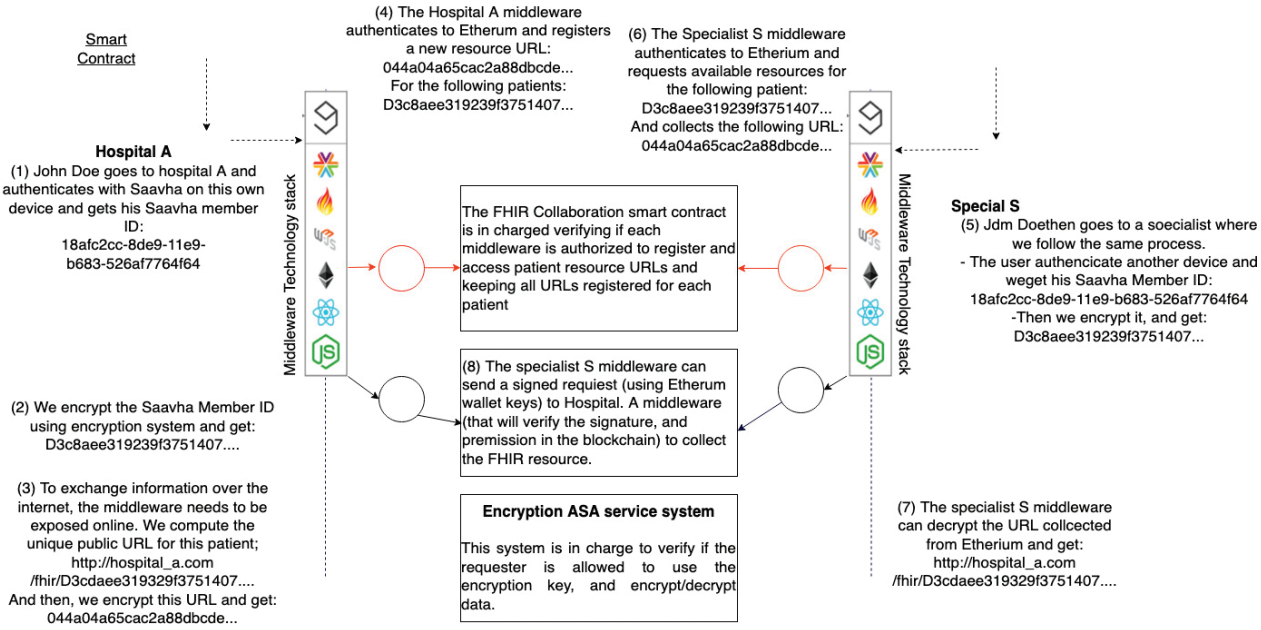


*Figure 2—User flow of OpenPharma Blockchain. AWS: Amazon Web Services.*

To become interoperable and retain CMS funding, EMRs must adopt the FHIR.[17] FHIR allows developers to create descriptive profile framework for existing resources that any system can read.[17] FHIR is based on RESTful web services and uses modular components as resources.[17,18] This allows software solutions with view only information exchange over HTTPS (Hypertext Transfer Protocol Secure). A resource may be a small packet of information that includes metadata, text, or data elements bundled to create a profile or a set of profiles with specific vocabularies for resources.[19] FHIR allows for standardization of URLs which applications can point to and retrieve information from over an HTTPS connection rather than exchanging files between systems using the insecure File Transfer Protocol.[17]

Building on FHIR standards, SMART on FHIR is a normalization for mapping to FHIR, which allows third-party applications to safely interact with an EMR without the need for vendor-specific integration.[19] SMART extends the functionality of FHIR by specifying what resources should be used when developing applications. Through SMART on FHIR, providers can capitalize on helpful applications without EMR integration, thus minimizing vulnerabilities or vendor lock in. In addition, SMART on FHIR provides a layer of security for patient data through a mature authorization model for third-party applications using the OAuth standards.[19]

The coupling of multilayer encryption and tokens secures patient identifiers on a public blockchain. The use of tokens allows for a smooth transition between services such as between servers or inside and 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) is used. This combination allows the users to verify their identity through SAAVHA. SAAVHA generates a separate patient-specific identifier authenticated using biometrics. The use of biometrics is revolutionary for verification and authorization. A person's voice is unique and changes over time. This gives it great potential as an identifier not dissimilar from a fingerprint. By speaking a predefined phrase into a microphone on the patient's device, SAAVHA verifies their ID and passes the authenticated member ID information off to Oauth 2.0, which grants a token that can be used to request access without passing on the user's protected identification information. SAAVHA uses machine learning to identify matching pass phrases. If two samples are too similar, a token will not be generated, and the account could be flagged if the threshold of failed attempts is exceeded. This safeguards against a recording of the passphrase being used to authenticate. SAAVHA also uses GPS location from the patient's device to compare with the provider's system GPS to ensure that the patient is present with the provider requesting access. This information also establishes a trusted device pairing for faster token retrieval during future visits and provides another layer of accountability for information access through audit trails.

**PROCESS FLOW**

First, prior to visiting their clinician, the patients should register with SAAVHA. Upon visiting their clinician (Hospital A), no special interaction with OBF is needed during the exam. OBF is designed to be launched as a lightweight and nonintrusive SMART on FHIR plug-in for the EMR. If patients are to be referred out to a specialist and would like to make their file

available, Hospital A would initialize OBF through their FHIR-enabled EMR; patients would then speak the predefined phrase set by SAAVHA and capture their voice for authentication.

Second, once authenticated, SAAVHA would return a member ID (e.g., **18afc2cc-8de9-11e9-b683-526af7764f64.** This member ID would never be made visible to the provider nor the patient but passed onto the OBF smart contract to store member IDs as a token (the SAAVHA member ID does not contain PHI). Only the relationship between the member ID and the patient URL generated by FHIR are saved in the smart contract, neither of which contain PHI. To ensure privacy, all information is then passed through multiple layers of encryption before being published to the blockchain.

**Encryption**

Figure 3 provides a summary of what data get encrypted and how the data are encrypted. Although public, information on the blockchain would not be easily accessible. Because of the sensitive nature of patient data, OBF uses redundant data encryption. All information would be encrypted and require matching digital key pairs to access data. Special permission scenarios must be established using key pairings. Every participant in the blockchain would have a private and a public key that would be cryptographically connected.[4] The public key would be available to view by everyone on the chain but access to any identifying data would be limited to those utilizing the corresponding private key.[4,12,20] This is handled through the smart contract[20] and a KMS. For further security and encourage adoption, only mappings between

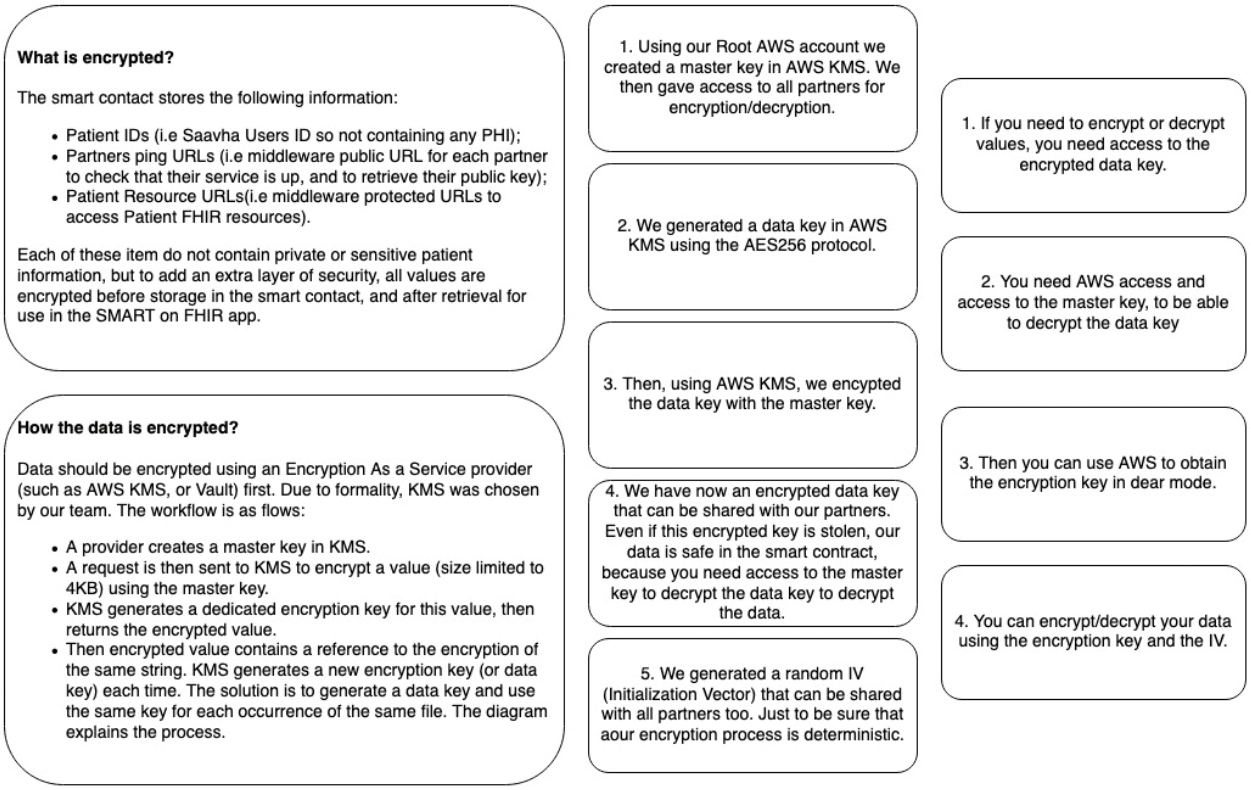


*Figure 3—Encryption steps. AWS: Amazon Web Services, FHIR: Fast Health Interoperable Resource, KMS: Key Management Service, SMART: Substitutable Medical Applications Reusable Technologies.*

member IDS and patient resource URLs are stored on the blockchain after encryption. Patient records are never stored on the blockchain; these remain at the originating EMR.

The smart contract stores the member IDs, partners' ping URLS (i.e., middleware public URL for each partner to check whether their service is working and to retrieve their public key), and patient resource URLs (i.e., middleware-protected URLs to access Patient FHIR resources). While none of these contain PHI, OBF encrypts them using a secured Encryption-As-A-Service provider Amazon Web Services (AWS) KMS to add additional layers of security before storing them in the smart contract and after retrieving them to use in the SMART on the FHIR app.

OBF generates and gives each provider a data key encrypted with the master key managed by KMS. When a provider wants to decrypt information stored on the blockchain, they first need to decrypt the data key by connecting to KMS. In the event of theft of the encryption key, the data are safe in the smart contract because of the required master key for decryption of the data key. In addition, a random initialization vector (also known as a nonce) is generated, which can be shared with all partners to be certain that the encryption process is deterministic. Random initialization vectors shield multiple usages of an encryption scheme with the same key. If the data are exposed without randomized initialization vectors, any potential agent may recognize a pattern or infer a relationship between encrypted data segments, which may leave data vulnerable to decryption through dictionary attacks. Once the member ID is passed to OBF from SAAVHA, the middleware can encrypt it and return a value similar to: **D3c8aee319239f3751407**.

**To Decrypt**

To decrypt information, providers would need access to the encrypted data key and have access to the master key. Only then would a provider be able to use KMS to obtain the encryption key in clear mode to decrypt data using the encryption key and the IV.

To exchange information over the Internet, the middleware needs to be exposed online. We compute the unique public URL for this patient using the encrypted member ID: **https://hospital_a.com/fhir/D3c8aee319239f3751407**. This is the URL to the patient's data in FHIR format, which any corresponding FHIR server would be able to recognize. Although the member ID is encrypted and protected, and we further encrypt the URL to return something similar to: **044a04a65cac2a88dbcde**.

**4.** Hospital A's middleware then authenticates to Ethereum and registers a new resource URL: **044a04a65cac2a88dbcde** for the patient: **D3c8aee319239f3751407**. To an observer, these values mean nothing due to encryption.

5. Once the patient moves to the next point of care, a similar workflow is used to authenticate, retrieve, and encrypt the patient's member ID. However, rather than just posting to the blockchain, the specialist is also requesting to collect information. No patient data are viewable without publishing information; a provider must announce a new relationship to the patient. Upon publication, the middleware then requests to collect information from all participants on the blockchain who have information for the patient: **D3c8aee319239f3751407**.

**6.** The Specialist's middleware authenticates to Ethereum, and requests available resources for the following patient: **D3c8aee319239f3751407** and collects the following URL:

**044a04a65cac2a88dbcde**. This information matches the information previously published by Hospital A. Records from multiple providers matching this unique member ID could be retrieved and viewed concurrently. This ability provides a more complete overview of the patient's medical history.

7. Once the information is found, the Specialist's middleware can send a signed request (using Ethereum wallet keys) directly to Hospital A's middleware. The smart contract will verify the signature and permission in the blockchain to collect the FHIR resource. This request is encrypted as well, hence the signature. The specialist's middleware can decrypt the URL collected from Ethereum and return a URL similar to: **https://hospital_a.com/fhir/D3c8aee319239f3751407**. Hospital A and the Specialist can now exchange FHIR resources between them securely.

8. Hospital A and the Specialist can use the embedded FHIR viewer to view the patient's records. Because the records never leave the source EMR, providers are free from delay related to downloading, storing, or adding them to their records.

## LIMITATIONS AND FUTURE WORK

OBF is limited by the aspect of patient consent. A clinician cannot collect information before the patient arrives; the patient must be present to give access to the file. This interaction may increase the length of visits, which may discourage adoption simply based on inefficiency. Because the patient's file does not leave the originating system, the clinician is unable to prepare for the visit prior to the patient's arrival. We plan to explore as to how to use mhealth app to integrate with OBF framework, so that the patients are able to authenticate themselves beforehand and provide permission to share data with providers as needed without the need to stop at the doctor's office.

Another limitation is the reliance of voice-based biometric for patient authentication. Such method may not work for patients who cannot speak, for example. We plan to explore integrating alternative biometric such as fingerprinting to resolve this in the future.

While Health Insurance Portability and Accountability Act of 1996 (HIPAA) was designed to protect the patients and empower them to have control over their records, it does hinder when it intends to help. The practice that no person should see more information than what is needed to do his or her job—called least privilege—is relatively common in business. OBF does not adhere to least privilege in the current iteration. To become more valuable, in future versions, OBF would need to have the ability to filter a patient file in order to omit viewing mental health data by the requesting clinician, as well as limit access based on user roles.

## CONCLUSION

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 data centers or a formalized information technology department are prohibitive both in cost and return on investment. Data standards such as FHIR are designed to encourage interoperability through uniform data structure. This allows for systems to organize and move relevant data more quickly.[21] 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.

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.

Just as the Internet evolved rapidly and changed communication, blockchain can grow to meet the needs of healthcare. The versatility and simplicity of 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.

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 is low. Without a strong directive from the government, with a mandated framework for infrastructure, interoperability may be a much longer and more painful process than is necessary.

Our solution requires participation of vendors at the very least to map to FHIR. By using open source technology already available, the cost of implementation would be relatively low. Because OBF is built using SMART on FHIR, integration into the EMR ecosystem should be unobtrusive. The only addition to the provider's day to day workflow would be the click of a button. The query, authentication, and encryption or decryption would be handled within the app. Security is at the forefront of any effort to share information. Through the use of encryption, authentication tokens, unique member identifiers, and file retention at the point of origin, patient information is as secure as possible to protect privacy.

**Funding Statement**: This research was partially funded by Healthcare Management and Informatics program at Kennesaw State University.

**Conflicts of Interest:** None

**Contributors**: Sweta Sneha was the overall research supervisor contributing from the perspective of a subject matter expert, research direction, outcomes, and editorial. Hossain Shahriar is Professor and Supervisor of Student Research Direction, technology, and manuscript development. Gracie Carter and Ben Chevellereau contributed to research, manuscript development, technical framework, and the development of proof of concept.

**REFERENCES**

1. Kim D, Kagel JH, Tayal N, Bose-Brill S, Lai A. The effects of doctor-patient portal use on health care utilization rates and cost savings. SSRN Electronic J [Internet]. 2017;(39). doi: 10.2139/ssrn.2775261
2, Linn LA, Koo MB. Blockchain for health data and its potential use in health it and health care related research. Proc ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, MD, USA: ONC/NIST; 2016:1–10.
3. NHE -Fact-Sheet [Internet]. CMS.gov Centers for Medicare & Medicaid Services. 2019 [cited 2018 Mar 10]. Available from: https://www. cms.gov/Research-Statistics-Data-and- Systems/Statistics-Trends-and-Reports/ NationalHealthExpendData/NHE-Fact- Sheet.html
4. Blumenthal D, Tavenner M. The "meaningful use" regulation for electronic health records. N Engl J Med. 2010;363(6):501–4.
5. Lapsia V, Lamb K, Yasnoff WA. Where should electronic records for

patients be stored? Int J Med Informat. 2012;81(12):821–7.
6. Bosworth HB, Zullig LL, Mendys P, et al. Health information technology: Meaningful use and next steps to improving electronic facilitation of medication adherence. JMIR Med Informat. 2016;4(1):e9. doi: 10.2196/medinform.4326
7. Opara-Martins J, Sahandi R, Tian F. Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. J Cloud Comput. 2016;5(1):4.
8. Chang JL. The dark cloud of convenience: How the HIPAA omnibus rules fail to protect electronic personal health information. Loy LA Ent L Rev. 2013;34:119.
9. Salahuddin MA, Al-Fuqaha A, Guizani M, Shuaib K, Sallabi F. Softwarization of Internet of things infrastructure for secure and smart healthcare. [Internet]. 2018;arXiv preprint arXiv:1805.11011. [Preprint].
10. Anjum A, Sporny, M, Sill A. Blockchain standards for compliance and trust. IEEE Cloud Comput. 2017;4(4):84–90.
11. CMS advances interoperability & patient access to health data through new proposals [Internet]. CMS. Center for Medicaid & Medicare Services; 2019 [cited 2019 May 10]. Available from: https://www.cms.gov/newsroom/fact-sheets/cms-advances-interoperability-patient-access-health-data-through-new-proposals
12. Leventhal R.Top Ten Tech Trends 2017: Blockchain's promise has healthcare innovators eager. [cited 2017 Mar 24]. Available from: https://www.healthcare-informatics.com/article/interoperability/blockchain-s-promise-has-healthcare-innovators-eagerPage
13. Sneha S, Varshney U. Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. Decis Support Syst. 2009;46(3):606–19.
14. Nye J. How blockchain could help boost healthcare security [Internet]. 2017 [cited 2018 Mar 1]. Available from: Healthdatamanagement.com
15. Dhanireddy S, Walker J, Reisch L, Oster N, Delbanco T, Elmore JG. The urban underserved: Attitudes towards gaining full access to electronic medical records. Health Expect. 2014;17(5):724–32.
16. Engelhardt MA. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Tech Innovat Manag Rev. 2017;7(10):22–34.
17. Bender D, Sartipi K. 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. doi: 10.1109/CBMS.2013.6627810
18. What Is Hl7 (health Level Seven International)?—Definition from Whatis.com. Available from: https://searchhealthit.techtarget.com/definition/Health-Level-7-International-HL7
19. Chaballout BH, Shaw RJ, Reuter-Rice K. The SMART healthcare solution. Adv Precis Med. 2017;2:213. doi: 10.18063/APM.v2i1.213
20. Ahuja SP, Mani S, Zambrano J. A survey of the state of cloud computing in healthcare. Netw Commun Technol. 2012;1(2):12.
21. Walonoski J, Scanlon R, Dowling C, et al. Validation and testing of fast healthcare interoperability resources standards compliance: Data analysis. JMIR Med Informat. 2018;6(4):e10870. doi: 10.2196/10870