Decentralized Electronic Medical Records

C C Darshan Thimmaiah
Computer Science & Engineering
Vidya Vardhaka College of Engineering
Mysuru, India
darshancc23@gmail.com

Disha S
Computer Science & Engineering
Vidya Vardhaka College of Engineering
Mysuru, India
dishas062@gmail.com

Deeksha Nayak
Computer Science & Engineering
Vidya Vardhaka College of Engineering
Mysuru, India
deekshanayak97@gmail.com

Diya B B
Computer Science & Engineering
Vidya Vardhaka College of Engineering
Mysuru, India
diyadechamma14.dd@gmail.com

Gururaj H L
Assistant Professor
Vidya Vardhaka College of Engineering
Mysuru, India
gururaj1711@vvce.ac.in

Abstract—*Today, hospitals and health systems continue to face many challenges in implementing, maintaining and upgrading their electronic health record systems. This paper discusses the various issues arising in the use of EHRs and their possible solutions. The aim is to securely store health records and maintain a single version of the truth. A probable solution is the use of blockchain. The different organizations such as doctors, hospitals, laboratories and other health insurers can request permission to access a patient's record, to record transactions and serve their purpose, on the distributed ledger. A platform can be built to securely store and share electronic health records by using the blockchain to create a distributed access and validation system which will help to completely replace the current centralized intermediaries. Thus providing a solution to today's health record problems.*

Keywords—*Electronic Health Record, Distributed ledger, Blockchain, IPFS, BigchainDB.*

I. Introduction

A very obvious problem that plagues the medical field is the nature in which medical records are stored. Electronic Health Records (EHRs) were never designed to manage the complexities of muti-institutional, lifetime medical records. The recent significant investments in Electronic Health Records (EHRs) were made for the purpose of improved patient safety, research capacity, and cost savings. However, the EHRs have failed to do so and most of these health systems and health records are fragmented across different organizations and do not share patient information. Recent news of security breaches has definitely put a question mark on this system. To avoid this, blockchain technology can be used to securely store health records. On a distributed ledger, different organizations such as doctors, hospitals, laboratories and other health insurers can add and view patient records with the patient's permission. By digitizing health records and empowering users countless industry Problems can be reduced.

II. Existing System

Over the past few years doctors, nurses and health professionals are limited in the level of care that they can provide. This is due to the inability to view the complete and accurate health record. Let's forget about the non-electronic records for a second, and just concentrate on the Electronic Health Record (EHR) for now. A record of a patient's medical details like history, physical examination, investigations and treatment stored in a digital format is called as an electronic health record (EHR). Every hospital has its own Record Management Software. Some store data locally in their databases, some use a cloud service provider and some store the data in a format compliant with insurance agencies. Most of the time, the user's data is on a server that belongs to the hospital or is rented by the hospital.

The major problems that this model causes are,

- Fragmentation of the patient's medical information across hospitals, private medical practitioners, and other m-health apps. As patients move between providers, they loose easy access to past records as their data becomes scattered across different organizations.
- Inability to transfer records from one hospital or application to another. Patients are not provided full access to their health records. Hence they have to get multiple tests done multiple times across multiple organizations.
- Inability to access vital medical information in case of emergencies.
- Data leaks and hospitals selling the patient's information to companies that benefit from it.
- Manipulation of data by hospital authorities.
- Unauthorized access to private medical data.

There is no doubt that data is the oil of the future economy. With machine learning algorithms becoming more robust, big companies are in need of more data. Social media platforms like Facebook are already facing the backlash of selling user data. Data is valuable intrinsically, and in the future, companies and big corporate may even pay users for their data. Hence data must be guarded like other valuables like gold, money, or cryptocurrencies are guarded. Because data is valuable in the exact same way. Medical data information, even more so.

III. Statistics

The statistics from October 2009, of healthcare data breach from when the Department of Health and Human Services' Office for Civil Rights has been shown in Fig.1. Only data breaches of 500 or more records are included in the statistics. Breaches still being investigated by OCR, as well as closed cases are included in these statistics. According to the statistics there has clearly been an upward trend in data breaches over the past 9 years. Since the records first started being published, 2017 has seen the most data breaches than any other year. There have been 2,181 healthcare data breaches between the years 2009 and 2017 involving more than 500 records resulting in the theft or exposure of up to 176,709,305 healthcare records. This equates to 54.25 percent of the population of the United

States. Healthcare data breaches are now being reported to be more than one per day.

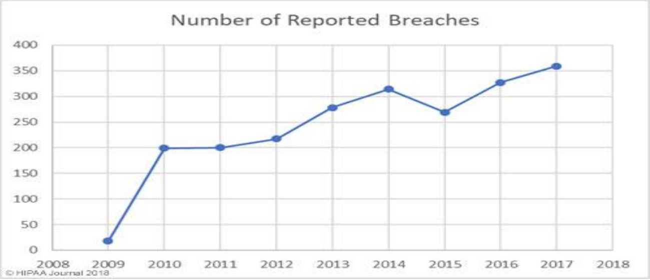

Fig. 1. Number of Record Breaches between 2009-2017

More healthcare data breach statistics showed in Fig.2 and Fig.3. These statistics show that, although health-care organizations now are much better at detecting breaches, hacking is still the leading cause of healthcare data breaches. The low hacking/IT incidents in the earlier years is probably due to the failure of organizations in quickly detecting hacking incidents and malware infections. Many of the hacking incidents between the years 2014 and 2017 occurred for many months, and in some cases years, before they were detected.

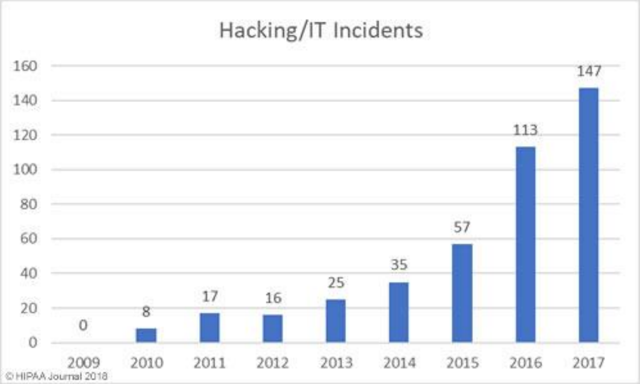

Fig. 2. Hacking/IT incidents Graph

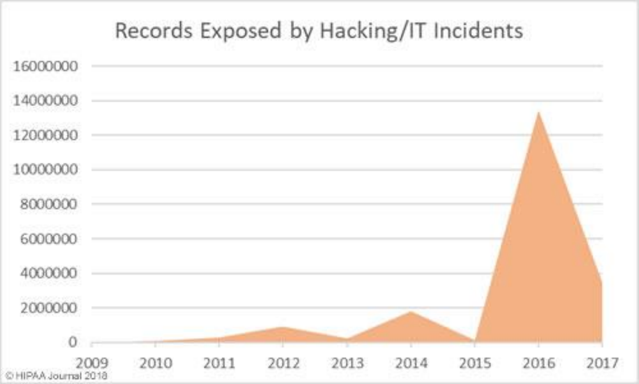

Fig. 3.Records Exposed due to Hacking/IT incidents

Healthcare organizations are now getting better at detecting internal breaches and also reporting these breaches to the Office for Civil Rights in time. While hacking is currently reported to be the main cause of breaches, unauthorized access to healthcare records or disclosure incidents are catching up and are in close second.

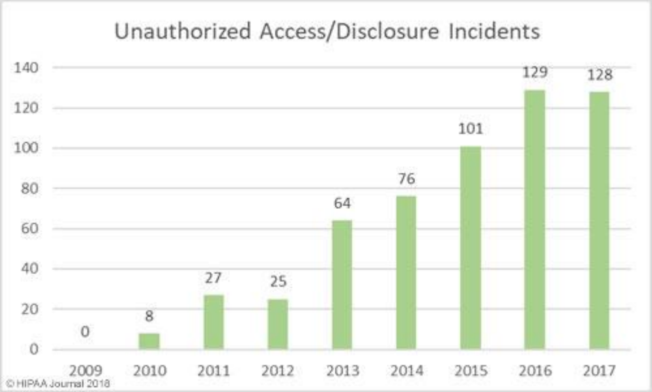

Fig. 4. Unauthorized Access/Disclosure Incidents Graph

IV. Proposed System

Billions of dollars around the world have already been secured by blockchain technology . So, it could be used to secure medical health records as well. The current EHR system can be challenged by using the strong security of blockchain technology, which offers a more technologically superior, and yet cost-effective solution. The proposed solution is to use the blockchain and create a distributed access and validation system to completely replace the current centralized intermediaries. This makes it possible for anyone to add medical information about the patient on a public database. But no one will be able to make sense out of anything until the patient gives them permission explicitly. All records created will be stored on a public blockchain, and cannot be manipulated at will. The technologies that can be used and how they can be implimented into our solution are listed below.

A. IPFS—The Interplanetary File System

The HTTP protocol is based on a client-server model, in which any content that the client wants to retrieve resides in a server, and the client asks for the content by first contacting the server. The server then responds by serving the client with the content that was requested.

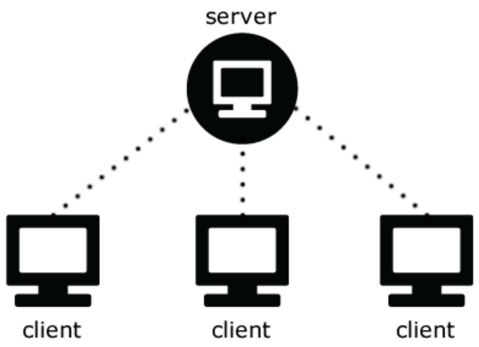

Fig. 5.Client-Server Architecture

One of the major drawbacks that it has, is fragmentation of data across multiple servers, in our case of medical records. Each hospital has the data on its own server, and to retrieve that data, the server needs to be contacted first. Sometimes the server may be even private or inaccessible. Hence IPFS can be used instead. This is how IPFS works: When u add a file to IPFS, each file and all of the blocks within it are given a unique fingerprint called as a cryptographic hash. Then the IPFS removes duplications across the network. Each network node stores only content it is interested in, and some indexing information that helps figure out who is storing what. When looking up files, the user is asking the network to find nodes storing the content behind a unique hash. Every file can be found by human-readable names using a decentralized naming system called IPNS.

The main concept is, instead of addressing content by the server it is stored on, address it by the content itself, or more specifically it's hash. And this content will be retrieved from nearest computer. Here IPFS will be used to store data. Meaning, if the patient just stays in one hospital, the patient's records stay there too. But if the patient moves to some other hospital and requests for their records, it will just follow them. As long as someone with their data is running an IPFS node, the data can be accessed from anywhere at all times.

B. Symmetric And Asymmetric Encryption

To make our records private such that only the ones that are authorized have access to it, it is needed to use some form of encryption. In symmetric encryption, there is a key also called a cipher that encrypts a document into a jumbled mess. To retrieve the original document it has to be decrypted it with the same key. A popular symmetric algorithm today is the Advanced Encryption Standard, or AES.

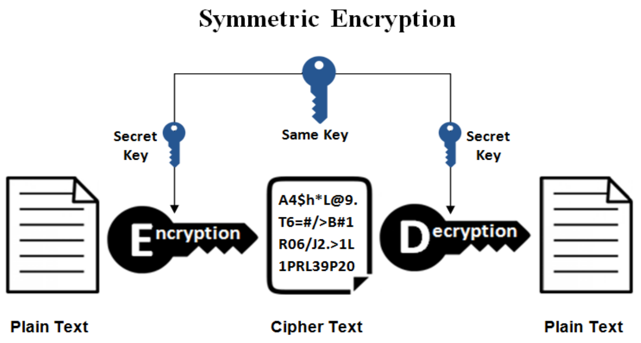

Fig. 7.Symmetric Encryption

Another encryption technique is the Asymmetric Encryption. In this method, there are two keys. A public key, and a secret key which is called as a private key. To encrypt a message the public key is used. However, to decrypt it, the secret key is needed. This means even the person who encrypted the message cannot decrypt it. The public key and the secret key are related mathematically, but the secret key cannot be derived from the public key. RSA is a very common Asymmetric encryption algorithm used by modern computers to encrypt and decrypt messages.

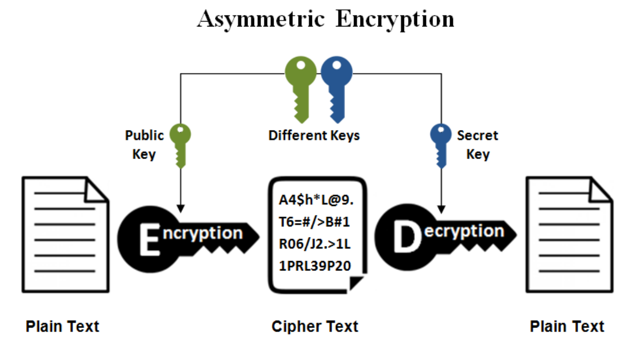

Fig. 8.Asymmetric Encryption

C. A Public Immutable Database

A public database that everyone can trust, because everyone or at least a lot of people have a copy of it. This will be used to store important information regarding our data, patients and doctors but not the data itself , as IPFS will be used for that.

V. Blockchain

In 2009 an anonymous author named Satoshi Nakamoto was the first ever to talk about and develop blockchain technology. Since its release, it has been used as the basis for thousands of cryptocurrencies around the world, including Bitcoin, Litecoin, Ripple, Ethereum and many more. It has also been recognized universally as the most secure technology amongst the available online database management technologies. Blockchain technology is a decentralized data storage that holds a public ledger of transactions. This ledger can record various transactions like property transfer, monetary transactions or even ballot storage. To ensure security and anonymity, all transactions that occur on a standard Blockchain are verified and signed with cryptography. This system uses elliptic curve cryptography, further improving the security. Simply put, the public ledger adds transparency and accountability while the cryptography provides security and privacy in the system. One of the most important attributes of blockchain technology is decentralization. A blockchain can be created which helps to securely store health records and maintain a single version of the truth. The different organizations such as doctors, hospitals, laboratories and other health insurers can request permission to access a patient's record to record transactions and serve their purpose, on the distributed ledger.

There are many options like BigChainDB, QTUM, Quorum, Hyperledger that can be used. But working on BigChainDB can be considered to be one of the most feasible options.

BigChainDB

BigchainDB is like a database with blockchain characteristics. It has high throughput, low latency, powerful query functionality, decentralized control, immutable data storage and built-in asset support. BigchainDB allows developers and enterprise to deploy blockchain proof-of-concepts, platforms and applications with a blockchain database, supporting a wide range of industries and use cases.

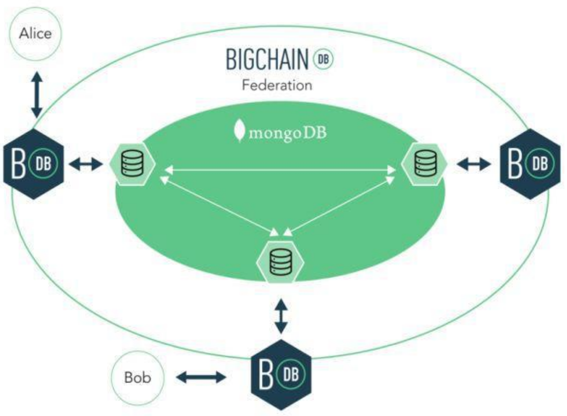

Fig. 10.Working of BigchainDB

VI. Process

Using the above mentioned technologies, medical data can be securely stored on an open database like the IPFS. None of the heavy data is stored on the actual blockchain, but is offloaded onto the IPFS. The process of making this work is given blow.

A. Declare the identity and a public key

Everyone on the network—the patients, the doctors, the apps first generate an RSA key pair. They keep the secret/private key a secret stored safely, while they make the public key public. Each participant will have declared a public key, while having the corresponding private key.

B. Health care providers generate data

This can be anyone who documents some data on the patient—A doctor, a laboratory, a fitness tracking app, or the patient themselves.

C. Encrypt the data using a random AES key

The AES symmetric encryption algorithm will be used to encrypt this data. First, a key is needed, that will be generated randomly. AES encrypt the report with this random key, to get an encrypted file. This file can be decrypted only with the previously generated random key.

D. Asymmetrically Encrypt the AES cipher for the patient

So anyone with the encrypted file and the random key can decrypt our file. The random key is now encrypted using RSA. The key is now decrypted and then the contents of the actual report are decrypted.

E. Store the encrypted data on IPFS and make the encrypted key public

Once stored on the IPFS, it generates a hash, which is unique to that record. Anyone with the hash can get the data. This is now stored publicly on the blockchain.

F. Patient views report

The patient is intimated, since a block has been added publicly. He can easily retrieve the hash code from the IPFS by just requesting for the file by that hash. Now to view, the patient, first needs to decrypt the AES key meant for him. He does so with his private key to obtain the random key that was generated in step C. The file is then retried from the IPFS using random key to decrypt it (using AES).

G. Patient gives permission for Doctor to view his/her data

Now if the patient goes to another doctor to get an opinion of the result, the new doctor can retrieve all information about the patient by just looking it up on the blockchain. He/She can retrieve every single report by it's IPFS hash. But, he/she can't view anything, because it's encrypted by our strong AES algorithm. So the patient needs to grant the doctor permission to view his/her report. The doctor's public key is on the blockchain. The patient just encrypts the AES key using random key and then RSA encrypts with doctors public key. Then the patient adds it on the block as a key meant for the doctor. Now the doctor, and only that doctor can decrypt the AES key using his/her private key, and then decrypt the report with that. The doctor, only has access to block that contains the report that the patient wants to show him/her. The doctor obviously knows that the patient has other medical information, since it's stored on the blockchain, but unless the patient grants permission, but adding a key for the doctor, it remains encrypted.

H. Patient wants to delete a record

The patient can add a approved:False flag to the block for this case. It will still remain on the blockchain forever and doctors will still be able to see it encrypted, but it will just indicate that the patient has refused this particular record. A history of everything is always maintained on the blockchain and nothing can really ever be deleted.

Emergency Data

If a piece of information is known to be vital during emergencies, that can be encrypted with 2 keys at the creation of the block instead of one. The emergency public key can be declared in the source code, or in some other open way. Also to make sure that this emergency address is not misused, an ethereum address with a significant amount, whose private key is encrypted with the emergency public key can be announced.This way, anyone who has access to the emergency account, is incentivized to protect the private key.

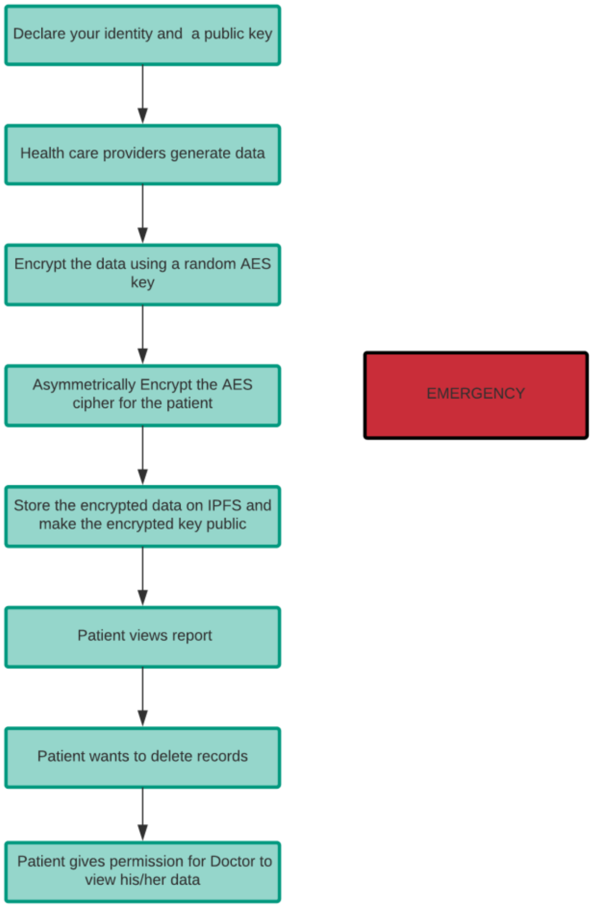
Declare your identity and a public key
Health care providers generate data
Encrypt the data using a random AES key
Asymmetrically Encrypt the AES cipher for the patient
Store the encrypted data on IPFS and make the encrypted key public
Patient views report
Patient wants to delete records
Patient gives permission for Doctor to view his/her data
EMERGENCY

Fig. 11.Flow chart for working of Procedure

VII. Conclusion

By using this solution, the current EHR system can be challenged by using the strong security of blockchain technology, which offers a more technologically superior, and yet cost-effective solution. The patients will be have complete access and control over their data and will also have the capability to provide access to various users, hence improving data security. Blockchain can be used and a platform can be built to securely store and share electronic health records to create a distributed access and validation system to completely replace the current centralized intermediaries. This will eradicate the problems of the current Electronic Health Record (EHR) systems like data fragmentation, data leaks, unauthorized access to the patient's data and many more. By digitizing health records and empowering users countless industry problems can be reduced.

VIII. Literature Survey

[1] Nir Menachemi, Taleah H Collum. Benefits and drawbacks of electronic health record systems. Risk Manag Healthc Policy. 2011; 4: 47–55. Published online 2011 May 11. Some authors have identified potential disadvantages associated with EHRs, despite the growing literature on benefits of various EHR functionalities. These disadvantage include financial issues, privacy and security concerns, and several unintended consequences. Financial issues, including adoption and implementation costs, ongoing maintenance costs, and declines in revenue, present a hurdle for hospitals and physicians to adopt and implement an EHR. Another potential drawback of

EHRs, which is an increasing concern for patients is the risk of patient privacy violations, due to the increasing amount of health information exchanged electronically. To overcome some of these drawbacks, policymakers have taken some measures to ensure privacy and safety of patient data.

[2] Steven R Simon, MD, J Stewart Evans, Alison Benjamin, David Delano, and David W Bates. Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study. J Med Internet Res. 2009 Jul-Sep; 11(3): e30. Published online 2009 Aug 6 . doi :10.2196/jmir.1164. Patients are enthusiastic about EHRs, recognizing its capacity to improve the quality and safety of health care. However, they are also concerned about its drawbacks which can result in breached privacy and misuse of health data. Policy makers will need to ensure that patients have access to concise educational materials and opportunities to engage in conversations about the risks and benefits of participation as the exchange of electronic health information becomes more widespread.

[3] Jeanne M Madden, Matthew D Lakoma, Donna Rusinak, Christine Y Lu, Stephen B Soumerai. Missing clinical and behavioral health data in a large electronic health record (EHR) system. Journal of the American Medical Informatics Association, Volume 23, Issue 6, 1 November 2016. Recent massive investment in electronic health records (EHRs) was predicated on the assumption of improved patient safety, research capacity, and cost savings. However, most US health systems and health records are fragmented and do not share patient information. EHRs inadequately capture mental health diagnoses, visits, specialty care, hospitalizations, and medications. Missing clinical information raises concerns about medical errors and research integrity. Given the fragmentation of health care and poor EHR interoperability, information exchange, and usability, priorities for further investment in health IT will need thoughtful reconsideration.

[4] Stephen O'Connor. Pros and Cons of Electronic Health Records. Published online February 6th, 2017. Whenever the users computerize records, they have to be careful about protecting the data from unauthorized access. It can be said that one con of adopting an EHR is that extreme diligence is required to shield sensitive data from cyber criminals and malicious hackers. Recent news accounts have underscored the danger of ransomware, where hackers install malware on the medical organization's servers. Their aim is to hold the data hostage until they receive money. In the meantime, patient details are unavailable, and work can slow down. There is also the potential for the public to learn about the data breach, ruining the practice's reputation.

References

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. BlockChain Technology Beyond Bitcoin.

[3] Mikel Aickin, PhD. Patient-Centered Research from Electronic Medical Records. Copyright © 2011 The Permanente Journal.

[4] Matthew J. Wills, Omar F. El-Gayar, Dorine Bennett. Examining health-care professionals' acceptance of electronic medical records using UTAUT.

[5] Alyssa Hertig. How Ethereum Works..

[6] Wei-Qi Wei, Cynthia L Leibson, Jeanine E Ransom, Abel N Kho, Pedro J Caraballo, High Seng Chai, Barbara P Yawn, Jennifer A Pacheco, and Christopher G Chute. Impact of data fragmentation across healthcare centers on the accuracy of a high-throughput clinical phenotyping algorithm for specifying subjects with type 2 diabetes mellitus. J Am Med Inform Assoc. 2012 Mar-Apr; 19(2): 219–224. Published online 2012 Jan 16.

[7] Debra Bradley Ruder. Malpractice Claims Analysis Confirms Risks in EHRs. February 9, 2014 - Patton McGinley.

[8] Rajiv Leventhal. Study: Inaccuracies in EHR Problem Lists Pose Problems for Risk Adjustment. January 22, 2018.

[9] Josh Benaloh, Melissa Chase, Eric Horvitz, Kristin Lauter. Patient controlled encryption: ensuring privacy of electronic medical records. Proceeding CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, Illinois, USA — November 13 - 13, 2009.

[10] Healthcare Data Breach Statistics- HIPPA Journal.

[11] Melissa Steward, Electronic Medical Records Privacy, Confidentiality, Liability.