SECURITY OF PEOPLE'S ELECTRONIC HEALTH RECORDS THROUGH INTERNET BASED THIRD-PARTY SYSTEM

Ezeoha B.U[1], Osuagwu O.E[2], Ekwonwune E.N[3], Agbakuru A.O[4], Amanze B.C[5]

[1]Department of Computer Science, Abia State Polytechnic, Aba, Nigeria
[2-5]Department of Computer Science, Imo State University, Owerri, Nigeria

Abstract: *This paper was motivated on the basis of finding a solution to the security concerns of patients about their electronic health records (EHR). Hence, the aim of this thesis is to provide the security of people's electronic health record (EHR) through an internet based third-party system. This concept will bring about a two-level authentication system devoid of a compulsory registration with an HMO, delayed implementation because of government's bureaucracy, and super admin's access privilege into a patient's record and or health center's record, as the technique that will resolve the issues with the most security techniques other researchers have suggested. The benefits of this concept include but not limited to better security of a patient's EHR, regain of patients' confidence in our health industry, interoperability of a patient's EHR, and patient-centrism.*

Keywords: Electronic Health Record, Security, Interoperability, authentication, patient-centrism, Information Security, barcode, Encryption, OTP.

1. Introduction

In today's world, everything is going "e" – electronic, and "tech" – technology: we hear of eCommerce, eBook, eHealth, eBanking, AgroTech, healthTech, etc. Hence, Health Information Technology (HIT) such as Electronic Health Record (EHR) is no longer a new concept to medical practitioners and centers that are going digital. According to [1], "an electronic health record (EHR) is a repository of electronically maintained information about an individual's lifetime health status and health care, stored such that it can serve the multiple legitimate users of the record." Electronic Health Records (EHRs) are digitized and stored for efficient patient management in hospitals or clinics, [2]. It is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting, [3]. An EHR is thus, a necessary electronic version of a person's comprehensive health information, from past to present which a medical practitioner or center would need when attending to the person. It is a record system that captures the health history of a patient as he or she undergoes treatments at different times and locations or hospitals.

More so, "EHR is interoperable from its architectural design: it can follow a patient if he or she switches providers", [4]. This capability to share data across health centers gives EHR systems an edge over other health information technologies, and therefore solves the problem of repeating processes such as health history data collection, each time a person visits a different hospital. Unfortunately, this interoperability advantage has its own security challenge: "this data-sharing component of EHR technology raises additional privacy and security issues beyond those created by EMR systems", [5]. The question of who accesses a patient's health information and how the access is gained have remained in the hearts of many. And [6] opined that "If patients' trust is undermined, they may not be forthright with the physician. For the patient to trust the clinician, records in the office must be protected. Medical staff must be aware of the security measures needed to protect their patient data and the data within their practices."

Therefore, a secured EHR can achieve a patient-centric health system.

This paper has been organized in sections. Section 1 contains a good Introduction of the topic; Section 2 talks about the Theoretical Framework according the scholarly opinions of other authors about this area of research; Section 3 and 4 contain the Summary and Conclusion, respectively. Section 5 is the Recommendation, while, Section 6 contains Conflict of Interest.

2. Theoretical Framework

The concern of patients about the privacy and safety of their electronic health records highlights the need for security. The security of health information of patients refers to the techniques which can be applied to safeguard or keep patients' sensitive information from unauthorized people. According to [7] Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. Also, [8] opined that Data security is any type of preventative measure that helps secure and protect data. The objective of data security for healthcare operations is to develop an effective and efficient plan to ensure their data and patient data are as secure as possible. [9] added that Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. They further added the definition Wikipedia gives, "Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms." In the words of [10], Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and availability of information. In health care, and for the purposes of this guide, confidentiality, integrity, and availability mean the following:

1. Confidentiality – the property that electronic health information is not made available or disclosed to unauthorized persons or processes.

2. Integrity – the property that electronic health information have not been altered or destroyed in an unauthorized manner.

3. Availability – the property that electronic health information is accessible and useable upon demand by an authorized person.

2.1 Security Concerns of patients' electronic health records (EHRs)

A number of studies that were aimed at investigating individual concerns for information privacy realized that they were essential in the realization of successful electronic health records technologies. [61] as cited in [11], confirmed that the confidence of an individual regarding the privacy and security of their medical records had a positive influence on their morale to establish an electronic health record. And, [44] in [11] further carried out a study whose results confirmed that there were existing concerns regarding health information privacy on the information privacy protective responses (IPPR) such as refusal of patients to give their personal information to health care providers, fabricating personal information of patients to medical facilities, requesting for the removal of personal information of patients, negative utterances to their friends, complaints issued directly to the medical facilities, complaints issued in an indirect way to a third-party organization.

[12] reported that research has shown that up to 90% of healthcare organizations have been the victims of at least one data breach in the last two years. In the last year alone, 253 data breaches led to the loss of more than 122 million health records. These breaches were caused by hacking/IT incidents (111,812,172 records), improper data disposal (82,421 records), data loss (47,214 records), theft (740,598 records), and unauthorized access (572,919 records). These breaches cost the US health sector $5.6 billion annually. Over the last 12 months, 1 in 3 Americans were affected by data breaches, with an average of 25.3 incidents reported every month over the first half of 2016. This figure rose to 39 data breaches per month over the last half of 2016, which translates to an increase of 55%. Some of the major companies that were compromised by cybercriminals during this period include Anthem Blue Cross (78.8 million records) and Premera Blue Cross (11 million customers).

More so, [11] further stated that close to half of the research participants in a study conducted by [6], as cited in their work, believed that exchanging their health information could worsen their health information privacy. And as cited in [11], [52] carried out a study in which half the respondents explained that they were worried about the security of their data because it had to travel through the internet; [10] confirmed that concerns regarding privacy negatively impacted the intentions to share their health information online; and a study conducted by [25] showed that concerns on health information privacy reduced the willingness of patients to allow health care providers share their medical data while using cloud computing technique.

2.2 Some Suggested Techniques for the Security of Patients' Electronic Health Records (EHRs)

In recent times, a lot of research has been made in the subject of security of patients' electronic health records; and it has come with questions that bother on the real life application and assurance of the suggested techniques. [51][30][32][48] as cited in [11] stated that Infosec Institute reported that the remarkable growth in the adoption of electronic health records in the recent years has not been protected by establishment of a cyber-security measure, thus subjecting the health care industry to a lot of damages from cyber threats. This report got a lot more support from other reports of Information Technology related incidents that were experienced in hospital settings. Furthermore in [11], a finding from Information Security Media Group in 2014, established that at least one security breach that affects less than 500 individuals has been reported in 75% of surveyed health care organizations in the US, and at least one incident affecting more than 500 individuals was reported by 21% of surveyed health care providers. [11] also said that the Healthcare Information and Management Systems Society in 2015 realized that 68 percent of surveyed health care organizations in the US submitted that they had recently experienced a significant security incident. These reported security incidents were from both insider threats (53.7%) and external threats (63.6% of health care organizations). The IT related security breaches could be more than the reported cases considering that there are other incidences that go undetected or poorly assessed, together with the likelihood of organizations to underreport security incidents. There are documentations showing that security breaches in healthcare can be very costly; for instance, Absolute Software Corporation which reported that cases of breaches in health care data costs hospitals as high as US $250,000 to US $2.5 million in settlement payments. This represent but a fraction of the overall financial burden of the incidents. Concerns of security and privacy together with fear of related liabilities hinders healthcare providers from using information and technology in improving their services. It is therefore critical that organizations improve their HIT security and privacy practices in the healthcare facilities as a measure to ensure that an effective health care is provided.

More so [13] added that as with any online digital format, concerns of breach exist. Internet hackers possess a digital power that frightens individuals looking to conceal sensitive data. There have been cases in which medical information has been accessed by unauthorized users. While this does not occur all too frequently, the occurrences are enough to plant some cynicism in the minds of physicians and patients. These are valid concerns. If confidential records end up in the hands of a person not privy to the information, the consequences can be overwhelming. Breach of medical records could lead to identity theft, which can destroy a person's finances, credit and reputation. Victims could seek litigation against the healthcare practice in which the breach occurred. If the breach affected multiple patients, the practice is headed down a long road of legal tribulations. This is why reputable records management companies have worked hard to provide top-quality security within their software in order to try to eliminate the risk of breach.

Hence, [8] opined that the types of healthcare data security solutions you should use will depend on the data storage methods used, the types of data you collect, how long you keep data, and so on. In general, you should have security measures in place that include security protocols for your patients, employees, contractors, vendors, suppliers, etc. Data access permissions need to be tightly controlled on a need-to-know basis. For instance, with patient insurance information and billing records, not everyone needs access to this data. Rather, you would want to limit access to only those responsible for processing insurance claims and billing patients for outstanding balances. The same is true with patient records that show their diagnoses, treatment plans, prescriptions, and so on. Only attending physicians and their nurses need access to this data. Other healthcare professionals may also need access, but that should be controlled on a case-by-case basis and limited to just the specific data they require. Some of the more common types of data security solutions you can use include:

1. **Data Backup and Recovery Solutions**

   You want to ensure your data are backed up daily to secure servers like a portable NAS server. Portable servers are ideal when you have multiple locations or want to ensure your backup is stored offsite in a safe and secure location.

2. **The Use of Data Encryption**

   Data encryption is vital when transferring data from workstations to servers, the internet, or cloud-based systems. Encryption is the highest level currently available and it absolutely should be employed.

3. The Use of Anti-Virus/Malware/Spyware Apps

You need to make sure your systems are protected from viruses, malware, spyware, etc. You should choose an appropriate app that best meets your needs and then keep it updated at all times.

4. System Monitoring Apps

There are several types of apps available that can monitor a wide array of different operations, processes, and procedures. You can use an app to monitor who is accessing, updating, creating, moving, and deleting files. You can use another app that detects potential data breaches. There are also apps to help identify unauthorized access, changes to user accounts, etc.

5. Enabling Multi-Factor Authentication

Since it can be difficult to rely on employees, contractors, vendors, suppliers, and others to use secure passwords, another way to protect your data is to enable multi-factor authentication methods. These methods require users to provide their username and password and then verify one or more additional items, such as entering a one-time use passcode sent to their email account or mobile phone.

6. Ransomware Protection

You will want an app that protects your workstations and servers from ransomware. This type of malicious attack locks you out of your own systems and holds them hostage until you pay a ransom to the hacker. Even after paying the ransom, there is no guarantee they will permanently restore your access to your data.

7. Employee Training

You should get into the habit of regular training sessions with new and current employees to ensure they are taking every precaution to protect patient records, data, and other vital information. You should get into the habit of regular training sessions with new and current employees to ensure they are taking every precaution to protect patient records, data, and other vital information.

In the words of [14], the number of Electronic Health Records (EHR) being lost or stolen is increasing year on year, despite the best efforts of healthcare organizations and the increasing strictness of HIPAA compliance. According to the HIPAA journal, January alone saw just over half a million records breached. Now, half a million records may not sound like much compared to other breaches, such as social media breaches, the sensitive nature of an EHR makes the breach potentially incredibly damaging. If an attacker gets hold of an EHR, or an EHR is sold on the black market, the potential risks of identity theft are huge. Some research even suggests that an EHR could be worth up to $1000 on the black market – making that half a million records breached in January suddenly take on a whole new value. [14] further outlined some techniques for the security of patient's electronic health record (EHR), as stated below:

1. Perform Regular IT Risk Assessments

The cyber-security market, especially in the healthcare sector, is a constantly evolving world of threats. To keep up with the advancements that attackers are making, and to ensure your evolving IT environment maintains the same levels of security, regular IT risk assessments are required. The main points are to ensure you know what the risks and threats facing your critical systems and EHR are, assess the areas where you might be vulnerable, identify and organize your data based on risk and take action to mitigate potential threats. It's not enough to perform this once a year, or even biannually. To truly ensure that your IT environment is one step ahead of the cyber-security threat landscape, IT risk assessments need to be performed as frequently as possible.

2. Patch and Update Regularly

Many cyber-security attacks, including the now infamous WannaCry attack, are able to wreak their havoc through exploiting unpatched our out of date medical devices. Many people outside of the healthcare industry may be surprised to learn that a vast majority of hospitals and pharmaceutical companies are running common operating systems, like Linux and Windows, making them just as susceptible to cyber-attacks as everyone else.

Probably one of the most effective cyber-security techniques is the religious and almost fanatical obsession with maintaining an up to date and fully patched software environment – including every device you use.

3. Clean Up User Devices

The healthcare industry is no stranger to Bring Your Own Device (BYOD) and the associated security risks. However, healthcare organizations do need to ensure that they have put in place the appropriate security controls, practices, rules, processes and technology to ensure that healthcare information access on personal devices is protected.

Ideally, healthcare organizations would not ever allow patient data to be accessed from personal devices. Virtual desktops can facilitate this, but they often over-extend healthcare budgets due to high back-end implementation costs. Therefore, mobile devices seem to be the way to go. However, there are ways you can ensure that BYOD doesn't lead to vulnerabilities in your data security. Mobile Device Management solutions offer a way of encrypting data accessed on mobile devices, deleting data in the event of lost or stolen devices, separating personal and professional data and much more. It's a must for those operating in a BYOD environment who are serious about their security.

4. Audit, Monitor and Alert

One of the biggest threats to data security in the healthcare industry, that often goes unaddressed, is insiders. Employees with privileged levels of access to the most sensitive information, including Electronic Health Records, are very often the cause of the biggest and most costly data breaches. This is because an insider threat can be malicious or accidental and go unnoticed for long periods of time due to its un-intrusive nature.

The only way to adequately defend against insider threats is to ensure that you have a way of continuously monitoring their activities and reporting on suspicious or unauthorized changes as quickly as possible. Unfortunately, the most common approach to this is through built-in log management functionality. Whilst this is better than nothing, it is nowhere near powerful enough to really affect your cyber-security posture. This is because it can be difficult to gleam meaningful information from raw logs, and the process of investigations can be both complex and time consuming.

5. Clean-Up Unnecessary Data

Often, organizations collect, store and process vast amounts of data unnecessarily. Data like this and stale accounts can present huge opportunities for hackers. Many compliance regulations, including HIPAA, require you to regularly review and delete unnecessary patient data for the sake of the security of that patient.

Furthermore, in identifying the advantages of electronic health record (EHR), [6] stated that "it supports and promotes the idea of patient-centrism." However, [6] explained that "Despite the key benefits of implementing Electronic Health Record (EHR) system, the bane of achieving a patient-centric interoperable health system is the access to Patients' health information. Who has right of access? When and why the access is made; and how the access is achieved, are some issues patients have with our health centers and staff. Thus, even if a national health system is achieved in Nigeria, the problem remains the security of a patient's health record. Today, there are cases of doctors, nurses, and pharmacists revealing their patients confidential health information/record to their friends and consequently, to the public without the consent of the patients. Some of such health information include but, not limited to HIV/AIDS and other STDs (Sexually Transmitted Diseases). Hence, questions and concerns about the security of a patient's health record cannot be ignored." They further proposed a security technique that would solve the problem of security of patients' electronic health record. Thus, [6] stated that "the solution to problem of achieving a patient-centric hybrid Electronic Health Record management system with strong security is **the integration of a two-level authentication/security system - the Barcode technology and encrypted Personal Identification Number (PIN) into the system.** This implies that every patient will have his health barcode and PIN generated at the point of registration with the HMO (or hospital as the case may be). Hence, this technique ensures a secured and patient-centric health record system such that nobody (doctor, nurse, clerk or any other hospital staff, etc) would be able to access a patient's health record unless the patient releases his barcode and PIN to him. In other words, a patient will be required to give his barcode and PIN to his physician for every healthcare service. The barcode can be enshrined into a patient's identification card, in printed form, or sent as text via short messaging system (SMS) or email. Whichever way it is communicated to the patient, the idea is that the patient must keep it personally confidential; hence, will know that anyone who has access to his critical health record must have gotten the access through him, one way or the other. In this way, hospitals and staff will be free from the age long blame of divulging patients' health information, and consequently, will regain the confidence of patients. Above all, health data security will be high and assured. This technique is close to the use of Automated teller Machine (ATM) card by bank customers.

2.3 Potential Setbacks with the Proposed Security Concepts

There are few but key security techniques suggested in section 2.2; others are mere conventional practices that do not really imply information security. The real security techniques mentioned include "Data Backup and Recovery Solutions, The Use of Data Encryption, System Monitoring Apps, Enabling Multi-Factor Authentication, the Barcode Technology and Encrypted PIN", and use of username and password. However, these techniques have potential setbacks which question their viability in the security of patients' electronic health records in this technology driven age.

Issue with Data Backup and Recovery Solutions

1. It can be weak to Man in the Middle (MIN) Attack: MIN is a type of attack that is lunched and exists within the time data is transported from a client system to the **backup** server. Hence, Data Backup and Recovery Solutions does not guarantee security of a patient's health record when a hacker decides to inject a MIN attack.
2. Regardless of the type of backup, online or offline, if the backup server and or the Virtual Environment created by the server is attacked, the backup would be gone.
3. Data Backup and Recovery Solutions is primarily for data recovery not a guarantee for security.

Issue with the Use of Data Encryption

There are many decryption software available today. These software are used by unauthorized users/hackers to decrypt coded information. Example of the Decryption software is the "John the Ripper". This software has recorded huge success in this area.

Issue with System Monitoring Apps

As good as these apps may appear, they come with a big setback:

a. They slow down the server given that every request must be monitored and verified. Hence, when there are multiple requests hitting the server, the speed of processing will drop drastically.
b. Consequently, they slow down user operations too. Take for instance, what happens in online bank and network transactions.

Issue with Enabling Multi-Factor Authentication

Phishing is a social engineering attack meant to obtain user sensitive information such as username and password, bank details like BVN (Bank Verification Number), ATM PIN, and CVV (Card Verification Value), patient electronic health record. Therefore, phishing can still be used to steal user sensitive data through emails and uniform resource locators (urls).

Issue with Enabling Username and Password

The use of username and password has become one of the reasons there is a lot of data/information security breach. In the words of [15], "Relying on passwords for security has become increasingly problematic. Devising and remembering a complex password for every account and website is virtually impossible on your own. Yet using weak and simple passwords is a recipe for data breaches, account takeovers, and other forms of cyberattack." He further gave instances of the type of passwords most people use as follows, "password", "123456," "Hello123," and "sunshine". He opined that "Some 20% of the passwords uncovered were the exact name of the company or a slight variation of it, such as the company name followed by a number or year."

More so, [16] stated that it is not a good idea to use username and a static password as the authentication m ethod for logins, since it dramatically increases the risk of unauthorized access to services and information. According to [16], Stefan Sundh, user authentication specialist at identity and security company Nexus Group, gives you the 13 reasons why passwords are not secure.

1. Users often reuse the same password for different services.
2. Many people do not change default passwords immediately, which means that it is easy for unauthorized people to gain access.
3. Passwords are often shared amongst users.
4. Users tend to keep the same password for a long time.
5. Password-cracking tools are getting *really* good at guessing passwords.
6. People often use too weak passwords.
7. Passwords are easily stolen through social engineering.
8. Passwords are sometimes sent over unsecure networks, which makes them easy to steal.
9. Organizations' password databases get hacked much more often than most people care to realize.
10. Users often write down passwords, for example on sticky notes.
11. Passwords can be stolen by malware equipped with key logger components.
12. If a password gets into the wrong hands, unauthorized people can access the service and its information without anyone noticing.
13. Organizations often fail to remove user accounts and their passwords when employees quit their jobs, which gives them access to information they should no longer have access to.

Issues with the Barcode technology and encrypted Personal Identification Number (PIN) that is suggested by [6]

The security technique that is suggested by [6], use of Barcode technology and encrypted Personal Identification Number (PIN) is no doubt a better security technique because it provides a very strong two-level authentication system. However, their idea has major setback in countries like Nigeria, which is the Registration with Health Maintenance Organizations (HMOs). Hence, the following questions pose a threat to the acceptance of this security technique:

i. Orientation of the people about HMOs
ii. Difficulty in getting people register with an HMO
iii. Must everyone identify with an HMO?
iv. Problem of independence of National Health Insurance Scheme (NHIS) of the government; hence, the potential problem of delayed implementation of the technique.

The acceptance of the idea of [6] has been affected the above stated questions; thus, patients' health record security concerns have continued.

2.4 How Can We Bypass This Problem?

One major observation in the idea of [6] which has raised the questions earlier stated is that the system does not run in isolation from the HMOs. Therefore, to bypass this setback, the researchers in this paper opine that the solution is the use of an internet based third-party system, and not HMOs. This internet based third-party system, which is an independent support system, is a web application that provides a common or central service platform to all health centers. The aim of this third-party system will be to develop the security of electronic health record (EHR) using PIN and barcode technology (QR code).

2.5 How Would this Internet Based Third-Party System Work?

This Internet Based Third-Party System will be developed to achieve its aim based on the following technical strategies/services:

1. Provision of an interactive and mobile-aware web based software (the hybrid): This new system, the hybrid EHR will not only help to centrally store the health history of everybody or patient in Nigeria, but will also help to eliminate the manual system and the interoperability issue of EMR system;
2. Provision of a hybrid model which is a two-level authentication system namely, encrypted Personal Identification Number (PIN) code and QR code system for each patient as security system that makes the hybrid EHR management system patient-centric. In this way, nobody will have access to any patient's record apart from the patient, using his PIN code and QR code. This will help eliminate the health information security concerns of patients.
3. Provision of a secured repository that keeps track of who accesses a patient's health record per time; thereby, aiding the legal system to bring to book any medical practitioner who violates a patient's health privacy right.
4. Provision of a platform which allows interested Health Maintenance Organizations (HMOs) recognized by the Nigerian National Health Insurance Scheme (NHIS) to be signed up to that common platform. It also accommodates patients and health centers that belong to HMOs to identify with them via their unique HMO code. This will ensure that a true hybrid and or national health system is run in Nigeria, such that a patient's EHR moves with him as he moves from one health center to another, and one HMO to another. It will also end the repeated process of gathering health basic information of a patient each time he visits a hospital.
5. Provision of a One-Time-Password (OTP) as a quick Short Message System (sms) to a patient in order to gain access into his user account and make access changes such as QR code.

"https://spehrecord.com/" is a sample framework which serves as the proof of concept in this paper.

2.6 Nature of the Internet Based Third-Party System

In order to achieve a better security system that will be independent of core government control, and isolated from HMOs, this internet based third-party system will be majorly characterized with the following:

a) Independent of government and HMOs: It will not be owned by either government or an HMO.
b) Independent of super admin access privilege to both patients' and health centers' records respectively: The third-party service provider will not have any sort of access into a patient's record and or a health center's record. If this is allowed, the security of patients' health information and patient-centrism will be defeated.

3. Summary

Irrespective of the advent of Health Information Technology (HIT), the rise in the tension among patients who question the security of their health sensitive data/information/records and its consequent effect on health centers have become a concern in the present day health industry. Sensitive health information include but not limited to HIV/AIDS, STDs (Sexually Transmitted Diseases) and mental cases. Government, health centers, and patients desire to have a system that will protect patients electronic health record (EHR) from unauthorized users. Thus, a two-level authentication system is on the front burner. The most proven security technique is the combination and authentication of a patient's PIN and QR code before access to his sensitive health data is revealed to anyone, doctor, nurse, pharmacist, the patient himself, etc. This technique has not only solved the security concerns of patients about their health information but has brought about a paradigm shift, patient-centrism. In this paper, several security techniques were reviewed, and their bottleneck ascertained. However, the security of patients' health record using PIN and QR code authentication technique by means of an internet based third-party system gives a better, stronger, and needed security solution and assurance, which is devoid of a compulsory registration with an HMO, delayed implementation because of government's bureaucracy, and super admin's access privilege into a patient's record and or health center's record.

This paper has thus far achieved its aim as stated, which is to propose the implementation of the security of patients' health record using PIN and QR code authentication technique through an internet based third-party system, as a solution to the problems of the security of patients electronic health record.

4. Conclusion

The transition from the present manual system and the Electronic Medical Record (EMR) system to Electronic Health Record (EHR) system using a patient's Personal Identification Number (PIN) and his QR code through an internet based third-party system has been presented in this paper. A patient's health data can now move with him through this new system without fear of being accessed by unauthorized persons; thereby eliminating repeated antiquated processes and interoperability issues. More so, patients and health centers get automatic QR code peculiar to each of them at the point of sign-up with the third-party system. Hence, the hybrid system at every level of operation requests for a person's Personal Identification Number (PIN) and QR code, and authenticates them before it logs them in. Thus, the system ensures that no doctor (or anyone) will have access to a patient's health information unless the patient releases his PIN and QR code to them. This is also the case among health centers given that no health center can access their "panel" unless their PIN and QR code are released for authentication. This system also eliminates the health data security concerns of patients; thus, making patients' health information system patient-centric.

5. Recommendation

It is recommended that health centers, hospitals and clinics, and pharmacies, adopt and implement this security technique holistically in order to rebuild and regain patients' trust.

6. Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Tang P.C. and McDonald C. J. (2006). Electronic Health Record Systems. Retrieved

from: http://eknygos.lsmuni.lt/springer/56/447-475.pdf

[2] IEEE. 2015. Data Types Managed Database Design for Dynamic Content: A database Design for Personal Health Book System. Retrieved from https://ieeexplore.ieee.org/document/7022451

[3] World Health Organization. (2012). Management of patient information Trends and challenges in Member States. Switzerland. Retrieved from

https://apps.who.int/iris/bitstream/handle/10665/76794/9789241504645_eng.pdf;jsessionid=618482E39FB2F873FE8136EC701534FB?sequence=1

[4] Ndukwe, Chidinma M. and Ezeoha, Bright U (2018). A Hybrid of Electronic Health Record (EHR) System and Health Maintenance Organizations (HMOs): A Sure Way to Improve Healthcare System in Nigeria,International Journal of Computer Science and Mathematical Theory ISSN 2545-5699 Vol. 4 No. 3 2018 www.iiardpub.org

[5] Holman T. [Editor]. 2016, FAQ: What are EHR systems and why are they important? EHR Implementation. Retrieved from https://searchhealthit.techtarget.com/tutorial/FAQ-What-is-EHR- technology-and-why-is-it-important (June 25, 2018)

[6] Laurinda B. H (2012). Electronic Health Records: Privacy, Confidentiality, and Security

[Online]. Available: https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09

[7] IBM (n.d.). What is data security?. Retrieved from

https://www.ibm.com/topics/data-security

[8] Ciphertex. 2020. Why Healthcare Data Security Solutions Are Important In The Healthcare Industry. Retrieved from

https://ciphertex.com/why-healthcare-data-security-solutions-are-important/.

[9] Sans. 2021. Information Security. Retrieved from

https://www.sans.org/information-security/

[10] hhs (n.d). Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. Retrieved from

https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf

[11] Ismail Keshta and Ammar Odeh (2020). Security and privacy of electronic health records: Concerns and challenges. Retrieved from

https://www.researchgate.net/publication/343422940

[12] University of Illinois Chicago. (2020). How Secure Is Your Data? Assessing and Mitigating Risks for Electronic Health Records. Retrieved from

https://healthinformatics.uic.edu/blog/how-secure-is-your-data-assessing-and-mitigating-risks-for-electronic-health-records/

[13] Ironmountain. 2021. Electronic Health Records Security and Privacy Concerns. Retrieved from https://www.ironmountain.com/resources/general-articles/e/electronic-health-records-security-and-privacy-concerns

[14] Philip Robinson (2020). 5 Ways to Secure Electronic Health Records. Retrieved from

https://www.lepide.com/blog/5-ways-to-secure-electronic-health-records/

[15] Whitney (2021). Lance Whitney (2021). How weak passwords could put your organization at risk. Retrieved from

https://www.techrepublic.com/article/how-weak-passwords-could-put-your-organization-at-risk/

[16] Nexusgroup. 2017. “13 reasons why passwords are not secure”. Retrieved from https://www.nexusgroup.com/why-passwords-not-secure/