Security, Privacy Challenges and Available Countermeasures in Electronic Health Record Systems: A Review

Adetayo Folasole1, Oluwasegun Solomon Adegbuyi1, Oluwaseun Isaiah Ekuewa2,*, and Patience Emanre Eshua3

ABSTRACT

Electronic Health Record (EHR) systems have revolutionized the healthcare industry by enabling the efficient storage, retrieval, and sharing of patient health information. However, the widespread adoption of EHR systems has also engendered a myriad of privacy and security challenges that must be spoke to guarantee the privacy, integrity, and accessibility of sensitive patient evidence. A range of countermeasures has been implemented to reduce the risks associated with EHR data privacy and security. These include contact switch tools that limit data access to approved operators, as well as advanced encryption methods like Identity-Based Encryption and Attribute-Based Encryption, specifically tailored for securing EHR data in cloud environments. By employing these protective measures, healthcare providers can enhance the safety of sensitive patient information while adapting to the dynamic digital landscape.

Keywords: Electronic Health Record (EHR), Privacy & Security Challenges.

1. Introduction

Consequently, an excessive concern in moving from paper-based health proceedings to electronic health records (EHRs). These exertions are predominantly being made by self-determining establishments. Electronic health record (EHR) systems have become essential tools for managing patient health information. EHR systems have improved patient care, clinical decision-making, and healthcare service delivery. EHR systems, according to [1], were first used in the 1960s for patient registration, admission, accounting, and management. They have subsequently been extended to help share and manage patient medical information. These changes, according to Grana, are more efficient, safer, and error free than paper recordkeeping. Conversely, the latest suggestions that unified health records offer numerous advantages [2], some of which comprise: a decrease in expenses, better-quality of care, the elevation of evidence-based medication and greatest keeping and flexibility. In order to attain these advantages, EHR systems essentials is to fulfill definite requirements in terms of data entirety, flexibility to disaster, great obtainability, and the reliability of safety strategies [3]. The prospective benefits of the e-health system have been measured over latest periods. Nevertheless, because of its numerous encounters, the prevalent procedure of e-health system is still at an initial stage. Understanding safety as well as privacy concerns are important issues in e-health system. The opinion that rules the patient–physician relationship is sight as privacy. Patients are obliged to stake essential information with their physicians. Conversely, they may not disclose important information as admission of some information may outcome in social stigma and discernment [4]. Over time, EHR systems have come into common use, due to decreases in costs, standardization in recordkeeping protocols, and governmental adoption of and support for EHR. The EU and the U.S.A federal government use and promote the use of EHR. U.S.A initiatives for promoting EHR include the enactment of the Health Insurance Portability and Accountability Act (HIPAA); the creation of the National Coordinator for Health Information Technology (ONC); the ONC’s National Health Information Network (NHIN) for sharing patient information; the 2009 United State of American Recovery and Reinvestment Act, which allocated $190 million to...
digitize health records; and a 2014 mandate that directs U.S. health providers to adopt EHR.

According to [1], the primary motivation for EHR is the enhancement of healthcare quality. Healthcare professionals can make better diagnoses and treatment decisions and do more to track and correct medical errors when they have access to current and accurate patient health information. EHR, moreover, can enable patients to move between health providers more easily to better manage their health and find social support groups.

However, EHR systems have also created data privacy and security challenges that must be addressed to confirm the discretion, reliability, and accessibility of sensitive patient information. This survey reviews these challenges, together with countermeasures for addressing them. It explores security threats, vulnerabilities, and risks of EHR systems and the effectiveness of existing security measures.

The EU’s aim is to distribute patients’ EHR data/information with the intention of “Free Movement” and of gaining value and effective health caution [3]. Nevertheless, there has been actual little action in strategy improvement containing many substantial privacy challenges elevated by a swing from a principally disengaged, paper-based health record system to one that is combined and electronic [6]. Furthermore, the developments in Data and Transport network Technologies take lead to a condition in which patients’ health data are challenging new safety and confidentiality extortions [8]. The three vital safety objectives are [7] privacy, reliability and accessibility. The safety of particular information is critical in the health sector, and it is thus essential to confirm the privacy, reliability and accessibility of personal health information. Agreeing to the ISO EN13606 merit [8], privacy denotes the “procedure that guarantees that information is available only to those approved to have admission to it”. Integrity means the responsibility to confirm that information is precise and is not reformed in an unapproved style. An integrity of health data need to be secured to safeguard patient safety, and one significant constituent of this security is that of confirming that the information’s total life cycle is fully auditable. Accessibility states to the “assets of accessibility and usability upon request by an approved identity”. In efficient healthcare delivery, the availability of health data is also essential. Informatics systems in Health must persist operational in the surface of usual calamities, denial-of-service attacks, and system failures. Safety also includes responsibility, also known as people’s right to condemnation or request why something happened.

Health data is also observed by several as being amidst the most intimate of all kinds of individual evidence. Defending this discretion is consequently vital if the confidentiality of focuses of care is to be preserved. Privacy comprises admittance control against any party not approved to access the information, and has been explained as “the assertion of personalities, collections, or organizations to regulate for themselves when, how, and to what magnitude information about them is connected to others” [9]. Privacy and safety in EHRs can be extremely susceptible by hackers, viruses, and worms. Several records of unintentional damage or the theft of delicate medical data have seemed in recent years [10], [11]. In the security and privacy structures that EHR systems have might be dangerous if these threats are to be challenged and procedures to expand the data protection of EHRs are to be implemented. With respect to many studies carried out, regarding data safety and privacy have been looked into. Recently, records analysis stated that each year there are up to 25 million required approvals for the admission of health proceedings in the U.S.A [12]. Likewise, in studies shown in New Zealand, Germany, and Denmark [13]–[15], informants estimated their data safety concerns as concerns EHRs. People are also mindful of the possible threats that EHRs may have. Individuals can choose whether to share or not to share their health-related data with institutes and health care authorities in Austria [16]. To alleviate these disquiets, organizations such as the Certification Commission for Healthcare Information Technology (CCHIT) bid a specialized database that shields a demanding scrutiny of, amid other things, safety features centered on existing principles [17], which is mainly significant for the U.S.A. CCHIT has been attesting the technology since 2006. Condition that access to EHRs is an important next strategy in initiating patients in their development in the health system [18]. Conversely, this unlocks fresh security challenges. Issues concern about both individual and entities’ admittance stages to patients’ EHRs. A patient’s EHR might be disjointed and manageable from some sites (by going to see different doctors’ offices, clinics, workers, etc.). Disclosure of information to unauthorized persons or companies, could cause security threats in some of these health data systems therefore, the need for protection against influences, unapproved right of entry and misuses, which comprises captivating into justification of confidentiality, dependability, verification, accountability and obtainability issues [19], [20]. EHRs also have complications in upholding data confidentiality [21], to the degree that managerial operators could sample access information without the patient’s clear permission [22].

2. Reviews

In [23] discuss strategies for protecting the privacy, security, discretion, and accessibility of EHRs. The authors define data privacy as a personality’s right to release confidential data. Such as privacy threats, data breach, can lead to the unauthorized sharing or transferring of health records, such as medical history, personal information, and financial information. Potential harms from data breaches include identity theft, financial fraud, and loss of privacy.

Reference [23] define data security as protecting personal information from unauthorized access. Threats to data security include the use of ineffective access controls to protect EHR systems and the use of mobile devices to access EHR systems, as these devices are often less secure than desktop computers.

Reference [23] equate confidentiality with limiting access to information to those who are authorized to have it. Confidentiality can be maintained by means like data encryption and system access control. Encryption is often used for data sent through an exposed network but is less often applied to data on media storage or mobile devices.
Availability is the need to ensure that a system can be accessed when an authorized user needs to use it. It encompasses various factors such as scalability, resilience, and the ability to recover lost data in unforeseen circumstances.

Measures for assuring the privacy and security of current EHR systems can be classified as administrative, physical, and technical protections. Administrative protections involve procedural safeguards, including conducting audits, appointing a designated information security officer, and developing contingency plans. Physical safeguards involve physically protecting health information software or hardware from unauthorized access, using devices like keycards and security cameras. Technical protections include defenses against attacks on a system’s required functionality, such as encryption, firewalls, user authentication, and virus scanning. Firewalls are mechanisms for limiting access to an organization’s networks. They act as a barrier between EHR systems and external networks, monitoring and controlling linkage traffic flow in order to prevent unapproved admission to systems, data breaches, and damage from cyber-attacks. For authorized users, firewalls enable secure remote access via VPNs or encrypted connections. Firewalls also generate logs of network activity that can help organizations detect and avert potential threats to EHR security.

User authentication helps to protect data from unauthorized access. Mechanisms for implementing password-based authentication should limit users to hard-to-guess passwords and promote frequent password changes. To ensure the effectiveness of password protection, users should log out of an EHR system once they complete their tasks.

Contemporary antivirus software can provide systems with real-time protection from various forms of malware, thereby protecting against disruptions in healthcare services. A best practice for antivirus software is to keep it updated to protect against emerging threats.

Reference [24] discussed strategies for securing EHRs. One risk to EHR data security is the use of unsecured and unreliable cloud environments to store HER records. This risk can be mitigated by encrypting data stored in the cloud. Strategies for data encryption include Attribute-Based Encryption (ABE) and Identity-Based Encryption (IBE).

IBE, an asymmetric cryptography protocol, generates public and private key pairs based on a user’s unique identity, such as email address or medical record number. According to [24], IBE simplifies encryption while providing fine-grained access control. It enables healthcare professionals to encrypt a patient’s records with a patient’s public key, thereby assuring that the patient will be the only person who can decrypt and access this data.

ABE, another asymmetric protocol, encrypts and decrypts data based on users’ attributes or characteristics: for example, their name, department, or employer ID (Fig. 1). ABE has been used to secure data in cloud storage, communication, multicast, electronic health records, and IoT applications. It can be used to ensure that only approved operators with appropriate attributes can right of entry sensitive content. According to [24], ABE offers adaptable, scalable, and precise access control in remote storage.

An ABE framework is initialized by a central authority (CA), which uses an inferred security attribute to produce a Master Secret Key (MSK) and a set of freely available Global Public Keys (GPKs). Following the framework’s initialization, the CA establishes its users’ private keys by integrating the GPK, MSK, and the users’ designated attribute. To use the framework to send a file, a sender encrypts the input file using the GPK. Any recipient of this encrypted file with the private key that was generated using S can then decrypt it.

According to [25], cloud computing facilitates the communication of health information and reduces administrative overhead by enabling healthcare service providers to centralize access to EHRs. Centralizing access can simplify the management of EHRs, provide faster access to a patient’s medical history, accelerate treatment, and potentially save lives. To maintain the privacy of cloud-based EHR data, that data can be encrypted before transmitting it to the cloud.

In [26], discuss the privacy and security of EHR data in private, public, and hybrid clouds. Public clouds are servers that are controlled by cloud providers, which store data in off-premises servers. This puts stored data like EHRs at increased risk from malicious actions like eavesdropping, denial of service, masquerading based on IP spoofing, man-in-the-middle attacks, and flooding. Private clouds are managed by hospitals and hospital-affiliated third-parties, which makes them less vulnerable to attack. Hybrid clouds combine resources from private and public clouds. Cloud providers often opt for hybrid cloud deployment because it offers a robust and cost-effective way to benefit from cloud computing while reducing the risks of public and private clouds. In order to assure the privacy of EHRs in hybrid clouds, [26]. Proposed PPX-AC, an access control model that delivers advanced protection against external and internal privacy threats. It offers fine grained access management for EHR data. It uses anonymization techniques to maintain data privacy while making data available for research.

Reference [26]’s Implementation of PPX-AC consists of three modules. One implements Angel Anonymization, a data protection technique that anonymizes sensitive information while continuing to allow its analysis and use. A second implements Policy Anonymization, which hashes access policies to prevent public cloud users and service providers from extracting its data. The third implements XACML-ABAC (Extensible Access Control Markup Language-Attribute-Based Access Control), a markup semantic that enables the specification of policy authorization frameworks in the public cloud. XACML-ABAC uses a private cloud as an operation center for anonymizing and controlling access to EHR data.

This approach relieves health organizations from handling these operations, and, by shifting processing to a private cloud, makes the public cloud less vulnerable.

Health organizations outsource EHR data to a private cloud environment. This environment submits the EHR data requests to the Policy Enforcement Point (PEP). The PEP transfers the permission inquiry to a context handler,
which translates the bid into XACML form and forwards it to the Policy Decision Point (PDP). The PDP request’s reserve/structure features from the framework manager, which in turn requests a request’s omitted attributes from the Policy Information Point (PIP) module. The PIP gathers the resources from EHR data, returning them to the context handler, which sends them to the PDP. The PDP reviews the access control policy and forwards the anonymized feedback to the Policy Anonymization module, where the policy is anonymized using hashing. The public cloud saves the anonymized policy and EHR data and sends an anonymized EHR access response to the private cloud entities.

Reference [27] proposes a new anonymization technique for protecting the privacy of electronic health data (EHD). Reference [27] defines data anonymization as the modification or removal of personally identifiable information from datasets to protect individuals’ privacy. The aim of anonymization is to confirm that data is usable for research, analysis, or other purposes without compromising the confidentiality of people’s information in the dataset. In contrast to existing approaches, [27]’s method can prevent identity disclosure even when attackers possess relevant background knowledge.

Along with details about a patient’s disease and treatment, EHD usually contains data such as names, ages, addresses, zip codes, identity and contact number, salary information, and patient history that can be used to determine patient’s identity. This data must be suppressed or altered to protect patient privacy. How to do this depends on the type of data. One type of data, Personal Identifiers (ID), includes distinct attributes like name and social security number that directly identify users and are removed during the anonymization process. This data must be removed. A second, Quasi Identifiers (QIs), are publicly available attributes such as age, zip code, gender, and designation that can be recycled to infer a personality’s uniqueness. Depending on the data’s use, QIs may be generalized, grouped, or suppressed. Finally, Sensitive Attributes (SA) include information about individuals that should be protected from adversaries. Examples of SA include disease, treatment history, and other sensitive personal information. SA can be adjusted, and then published with individual-level data.

Method proposed in [27] is intended to simplify data anonymization. Suppose a hospital has collected data that it will share with pharmaceutical companies for research into new drugs. To protect individual privacy, data must be anonymized before publication while retaining as much information as possible for researchers and minimizing privacy concerns related to background knowledge and linking attacks. To anonymize data that includes QIs and SAs, [27] introduced the following key steps:

1) Pre-process e-health records; by cleaning, organizing, and transforming raw electronic health data into a structured and usable format.
2) Rank users with the highest similarity based on QI values. Create equivalence classes using the privacy parameter.
3) Examine the values of each attribute in each equivalence class by displaying the data, then identifying and removing outliers through visual inspection. Anonymizing these equivalence classes may reveal more information about the actual data in certain cases.
4) Categorize attributes as numeric, character, or hybrid. Remove explicit identifiers, such as email addresses and postal addresses, before anonymization starts.
5) Replace the original attribute values with more general values. This can include splitting a numerical attribute's range into intervals and replacing all values in that interval with the interval's average value.

Reference [28] uses a case study to illustrate the use of medical blockchains to preserve the privacy of smartcard-shared EHR data. The authors define a medical blockchain as a decentralized digital ledger system that securely stores and manages data across a distributed network of computers. This system leverages blockchain technology features, such as decentralization, immutability, security, and transparency, to address the unique challenges faced in managing and securing healthcare data.

Reference [28]’s case study focuses on the use of medical blockchain to manage patient registration and diagnosis-related data. Initially, a patient must sign up for a smart card with the Health Care Authority (HCA), a department managing healthcare information with the Ministry of Welfare and Health. The HCA oversees smart card distribution and registration. Each smart card contains a given patient’s health data. Following registration, a medical professional can identify a patient using smart card at a hospital.

As part of registration, a patient submits Personal Identifiers (SSN, address, telephone number), Quasi-Identifiers (gender, blood group, age), and a Password to the Health Care Authority for registration. If the registration is approved, the HCA establishes a fresh smart contract account with a public and private key, as well as an address, then incorporates the registration parameters and patient address into the related smart card. These parameters are saved in the HCA data storage system before issuing smart card to the patient.

Reference [28] characterizes a diagnosis process as consisting of the first consultation, emergency situation and follow-up consultation. The first consultation involves a patient’s first visit to a hospital. During this first visit, the patient first logs in by inserting the smart card and entering a password to authenticate their identity. The system then displays the patient’s identifiers on the doctor’s computer. The doctor diagnoses the patient, generates an electronic health record (EHR), and signs it. The doctor obtains the patient’s social security number (SSN) and saves it, along with the registration parameters, in the hospital database. When prescribing medication, the doctor uses the patient’s identifiers to provide advanced treatment and avoid allergic reactions. After receiving a diagnosis, patients can choose to authorize the sharing of Electronic Health Record (EHR) with research institutions. If consent is given, the password must be entered, which allows the hospital to extract the relevant data for EHR de-identification. The de-identified patient EHR is then imported to a smart contract and publicized on the medical blockchain. Since the patient’s personally identifiable information has been removed from the EHR, privacy is fully guaranteed. Licensed researchers can access the health data through medical blockchain without contacting the hospital. Furthermore, the anonymity of the blockchain ensures data cannot be linked to a specific patient, and its immutability verifies the medical data’s accuracy. If patients need to consult a doctor at a different hospital, the doctor can use the patient’s address to locate the EHR and access the medical information without any delays. This process saves patients time and money.

For follow-up consultations, the patient inserts the smart card and enters their password. The diagnosis system then calculates the parameters and verifies the patient’s identifiers. Next, it checks the database to see if the patient’s electronic health record (EHR) exists and if information has been de-identified in the medical blockchain. If both conditions are met, the system displays the patient’s information to the doctor. If not, it only shows the patient’s identifiers.

In an emergency, such as comatose, patients need immediate treatment without completing the login procedure themselves. As a result, the healthcare worker can access the patient’s previous electronic health records (EHR). The healthcare worker inserts the patient’s smart card into the hospital device, allowing the diagnosis system to retrieve the patient’s parameters. The healthcare worker can then search for the patient’s EHR using the index parameter from the database. If the search results are supportive, the system sends identifiers (such as email and ID) to the doctor’s computer. If not, a failure message appears, indicating a first-time consultation patient.

2.1. Requirements for Privacy in Healthcare Systems

Numerous privacy and security necessities should be fulfilled to deliver the suitable smooth of privacy in EHR system. Many researchers explained more than twenty security necessities that were initiate on assessments such as [29], [37]–[40], [42]–[47]. Due to space restrictions, the most important requirements are listed:

1) Accessibility in control is the capacity to minimize and control the admission to possessions by approved users [29], [42]. It uses three different privacy and security requirements such as authorization, authentication and identification. Identification is not a unique safety challenge in itself, but its persistence is to recognize handlers. Consequently, it caused to affect the way a handler can be authenticated [43]–[45]. Authentication, in turn, offers assurance that the demanding information access is reliable and effective [29] likewise have the claims of identity upon accessing [42]. There should be assurance that the communication is with an approved personnel on the other side [43]. Lastly, the authorization procedure defines which quantity of data can be limited to an outsider upon the safety rules and policies. It is significant to reference that an appropriate admittance control tool should guarantee patient confidentiality and also offer decent stability between accessibility and privacy [37], [44] safety objectives.

2) Availability defined as the property of a system and reserve being available, functional and accessible upon request by approved personnel [37], [40], [42] whenever it is needed in healthcare system [46]. Guaranteeing availability also comprises averting service interruptions due to hardware limitation and shortcomings, power fluctuation/ouage, and system upgrading [38], [43].

3) Dependability on the other way round guarantees effortlessly retrievable medical information at any period
even if there are some challenges faced by failure node or the grid network complexity [40], [47]. Normally in many health cases, the inability to regain precise information is due to dangers produced by the network complexity, impeding the patient’s life. Fault acceptance is required for dependability.

4) Flexibility is mainly to allow unapproved partaker who is not on the accepted list to have the right to use specific data in an emergency case to protect the patient’s life. Incapability or avoidance of access or right to rules may threaten a patient’s life [40].

2.2. Security Attacks in Healthcare System

Healthcare systems are susceptible to infiltration by mischievous occurrences or deliberately from handler for their selfish interest. This damages the efficiency or weakens the performance of healthcare systems [30], [48], [49]. Explicitly, transparency in hospital network, insulin pump sensors, or patient’s health data can be hacked or taken by malevolent handler [41], [47].

Several threats to data collection level such as altering information, dropping some important data, or resending data messages have been caused by these act.

1. **Jamming Attack**: defined as the interference caused by attacker’s radio signal with frequencies of the BAN (Body Area Networks). This causes segregating and averting sensor node within the threshold of the hacker’s signals for transmitting or receiving any information among the affected nodes and other transmitting end as elongated as the jamming signal keep occurring [31].

2. **Data Collision Attack**: occurs when two or more nodes try to transmit concurrently. Likewise, it can be considered as jamming attack as soon as a foe deliberately produces additional impacts by means of transmitting repeated information on the network [32], [33]. In a situation, that which the frame header is transformed due to an impact, the error scrutiny mechanism at the reception perceives that as an error and rejects received information. Also, a change in the information structure header is a risk to data accessibility in the BAN [31].

3. **Data Flooding Attack**: Here, the attacker frequently transmit many requests to the targeted network for linking until all the power of its capacity reaches a determined boundary, causing a flooding attack [34].

4. **Desynchronization Attack**: This type of attack, the hacker’s interferes with the information between sensor nodes by duplicating it several times by means of a counterfeit classification number to either transmitting or reception endpoints of an active linking, which leads the WBAN to an immeasurable cycle, causing the sensor nodes transmit information again and wastes their energy [32], [34].

5. **Spoofing Attack**: This is where the hacker’s targets the transmitting messages to achieve numerous interruptions including spoofing, changing, or repetition of the transmitting information, causing a complicated network by generating transmitting loops [35].

6. **Selective Forwarding Attack**: this happens when the hacker’s malevolent node in an information flow path frontwards designated information and ignores others. The destruction becomes severe when these malevolent nodes were situated closeness to the base station [36].

3. Conclusion

Data associated with patients should be preserved and secure in health provider servers in order for physicians to provide appropriate treatments. To guarantee safe storage and accessible management, in this paper, dispute were made regarding the safekeeping against the attacks in healthcare system alongside with the suggested security models that object to averting such attacks. Precisely, threats and challenges were classified into three kinds depending on the its appeared stages/level of the healthcare system, for instance: at transmission level; data collection level; and at storing level. These attacks may result in numerous threats such as releasing some significant data, interfering communication, changing information, or sending extra signals to block the base station and increase networking traffic.

After that, we concisely discussed a novel context-aware accessible control security model that is subsistence to the security essentials of healthcare systems and provides fine-grained access control. The model comprises of several modules, each of which is responsible for taking a diverse type of task. This modular design aims at unpretentious and effective accessible control results liable on the patient’s status quo and the handler’s allocated roles.

References