*International Journal of Engineering Applied Sciences and Technology, 2019*
**Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 35-47**
Published Online July 2019 in IJEAST (http://www.ijeast.com)

# SECURITY AND PRIVACY DETERMINANTS FOR A SECURED CLOUD-BASED ELECTRONIC HEALTH RECORD SYSTEM

Okal Christopher Otieno
Department of Information Technology
Mount Kenya University
P.O Box 342 -01000- Thika, Kenya

Harriet Tsinale Loice
Department of Information Technology
Mount Kenya University
P.O Box 342 -01000- Thika, Kenya

*Abstract*— **One of the technologies that have become widely adopted by healthcare institutions is the Electronic Health Record (EHR) systems. According to the International Organization for Standardization, an EHR system is a digital platform that allows multiple authorized users to store, access, and exchange patient related information. EHR systems fall under to main categories, namely; client-server and cloud-based HER. Each of these kinds of systems has unique pros and cons. The primary objective of EHR systems is to ensure timely access to patient records and information as well as integrated, efficient, and quality health. However, there are various risks associated with cloud-based platforms. In an attempt to understand these risks, the papers explore the available literature regarding cloud EHR systems as well as their risks. The review also examines the measures that medical care institutions, as well as cloud service providers, should take to enhance the privacy and security of medical records stored in cloud EHR systems. The results indicated that cloud base EHR systems are prone to multiple security issues such as hacking and leakage of information which compromise the privacy, security, and confidentiality of patient information. However, there are various measures that organizations and cloud service providers can take to minimize the prevalence of privacy and security issues in cloud EHR systems. The common measures include carefully selecting a reliable service provider, putting in place system features that will enhance security and privacy, carefully planning out the process of moving records from traditional storage methods to cloud-based servers and training of employees and patients in regards to the privacy and security of cloud-based EHR systems**

*Keywords*— Electronic health record systems, On-premise health record systems, Cloud-based health record systems, Cloud Server, Data Security, Internet.

## I. INTRODUCTION

The world has become more oriented toward technology. Most processes that once required human attention have become automated over the years. Technological advancement has become more rampant as a result of increased innovativeness, globalization, and the rise of internet technology [1]. Various techniques have also been adopted in the field of medical sciences and healthcare provision. Most of the technological advancements in the hea.th sectors are tailored towards improving customer satisfaction as well as healthcare delivery and outcomes. Furthermore, most healthcare institutions are in a quest to enhance the quality of care delivery.

In this regard, one of the technologies that have become widely adopted by healthcare institutions is the Electronic Health Record (EHR) system [2]. According to the International Organization for Standardization, an EHR system is a digital platform that allows multiple authorized users to store, access, and exchange patient related information. Such information may include, the patient’s past and present conditions, medical prescriptions, and medical diagnoses among others [3]. The primary objective of EHR systems is to ensure timely access to patient records and information as well as integrated, efficient, and quality healthcare provision [3]. EHR systems have had various significant impacts on improving healthcare delivery [4]. Some of the advantages of these systems include a reduction in medical diagnostic errors, ease of access to medical information, a decrease in other medical errors such as providing wrong prescriptions to patients. Additionally, EHR systems also promote collaboration among various medical stakeholders, thus improving decision making and consequently, healthcare delivery [5]. However, these systems are also associated with multiple cons, such as risk in the occurrence of medical malpractice claims. Cases of malpractice are more common during the initial stages of EHR adoption and implementation.

Apart from increasing the likelihood of the occurrence of medical malpractice claims, EHR systems also influence the outcomes of such litigation. As opposed to traditional health record systems, information stored in EHR systems is well organized and easily retrievable. Moreover, it is easy to track the activities of all individuals that use the system. In this regard, EHR systems can easily provide information that may be used to either hurt or support a medical malpractice case. Furthermore, some EHR systems provide medical suggestions to medics and aid them in decision making. However, the actions taken by physicians or any decisions made are ultimately their liability [6]. In this regard, EHR systems are also likely to increase the occurrence of errors in the healthcare provision process. According to a study that was published by the Journal of the American Medical Association, EHR systems were found to be associated with 22 different types of errors. Some of the common errors include prescription error and dosage errors [6]. Moreover, most EHR platforms have predefined and fixed ordering systems, which increase the likelihood of making wrong orders in situations that require order customization. Lastly, EHR systems are also prone to cases of security breaches and cases of information leakage, which may lead to patients' medical information falling into the wrong hands.

EHR systems fall under two main categories, namely; client-server and cloud-based EHR) [7]. In the client-server system, information is stored in servers and systems that are controlled by the specific institution that utilizes the platform. On the other hand, cloud-based systems store data in external servers and are controlled by third-party institutions [8]. Data stored in cloud servers can be accessed through the internet [9]. The challenges associated with the client-server EHR records are motivating institutions to adopt the cloud-based platforms [10]. However, despite the high preference for the cloud-based EHR systems, there are various risks associated with transferring patients' records to cloud servers that are hosted by third parties as well as multiple measures that healthcare organizations and cloud service providers should take to minimize these risks.

## II. PROBLEM STATEMENT

In recent years, there has been an upsurge in security issues in regards to data stored in cloud systems mainly in the financial sector [11]. However, Medical institutions have begun to adopt cloud-based electronic health record systems, and thus, the security concern has shifted to this industry. The healthcare industry is presently considered as one of the largest targets for hackers and other cyber criminals who might be interested in accessing patient data. Studies reveal that approximately 60% of healthcare institutions have resulted in the use of cloud-based systems [12]. The primary reason behind this widespread adoption of these systems is due to the cost efficiency associated with their implementation and maintenance as compared to self-managed systems or on-premise EHR systems. Despite this increased concern, most healthcare organizations have not put in place measures to secure their data. Additionally, most organizations have failed to pay enough attention to the security concerns when transferring information from manual systems or on-premise servers to cloud-based systems. Protecting the privacy of patient information should be one of the primary concerns for healthcare institutions. As cloud-based systems are exposed to multiple vulnerabilities as this paper will reveal, it is important for healthcare institutions to understand the potential security risks associated with these systems, factors that may increase vulnerability to these risks, and the measures that healthcare organizations, as well as cloud service providers, should take to enhance data security. Therefore, this study will provide information that will enable healthcare institutions to weigh their options on the two main types of EHR systems, the security risks associated with Cloud EHR systems and measures that should be taken before adopting cloud electronic health record systems. The paper will also explore the literature on emerging issues regarding the security and privacy concerns of cloud EHR systems hence enabling medical institutions to take the right measures towards security enhancement.

## III. CLOUD-BASED VS. ON-PREMISE EHR SYSTEMS

Organizational EHR systems are housed in different environments; such habitat can also be referred to as the Deployment environment. The environment contains a collection of software, hardware, servers, and middleware, among other components that come together to make the system functional. The deployment environment can be simple or complex, depending on the nature of the system. The deployment environment can either be in-house or hosted by third parties externally. The deployment environment of a cloud EHR determines whether or not it can be classified as Cloud-Based or On-premise.

## IV. ON-PREMISE EHR SYSTEMS

As stated, before on-premise EHR systems or client-server systems are hosted by in-house servers which are operated, controlled, and maintained by the organization through dedicated people such as the IT personnel. The user organization has complete control of the system and is responsible for all aspects of design and maintenance. Such systems do not require an internet connection for the users to be able to access the information that is stored within the internal servers. Like most organizational systems, on-premise EHR systems have their unique advantages and disadvantages, as shown below.

## V. ADVANTAGES OF AN ON-PREMISE EHR SYSTEM

On-premise EHR systems are considered to be more secure than the cloud-based systems. High levels of confidentiality and privacy should be upheld when dealing with patient-related information; this ensures that such information does not fall into the wrong hands or it is not revealed to the unintended people. On-Premise systems are considered to be more secures since they are less prone to incidences of hacking or outside interference by third parties. Furthermore, on-premise EHR systems can easily be accessed even in the absence of an internet connection; this ensures that medical care providers can access the required information with minimal constraints or hindrances [13]. Additionally, on-premise systems are also not prone to unplanned interferences or interruptions arising from external activities such as software or system updates and maintenance by the hosting companies. The systems ensure that an organization can conduct its activities with minimal interruptions as well as to factor for disruptions in its operations since they can easily communicate and organize with the individual mandate to maintain such a system [13]. Additionally, on-premise EHR systems take less time to repair since individuals closely monitor them within the organization as compared to cloud-based systems where organizations have to liaise with the service providers in case of an unexpected breakdown which might be time-consuming [13].

## VI. DISADVANTAGES OF AN ON-PREMISE EHR SYSTEM

Despite the advantages listed above concerning on-premise EHR systems, there are various known disadvantages associated with such systems. Though the systems are secure and easy to access, they are demanding in terms of their maintenance cost. On-premise systems require frequent monitoring and maintenance by skilled and trained personnel [14]. This can be a huge challenge especially for upcoming institutions that do not have sufficient funds to bear the cost of maintenance or to hire sufficient and qualified people to oversee to the maintenance and operations of the system. Furthermore, on-premise EHR systems are expensive to purchase and setup [14]. The financial implication associated with acquiring such a system can be too high for medical care institutions. Apart from the huge financial impact, on-premise EHR systems also require a lot of space for server rooms and the needed infrastructure. This can pose a significant challenge, especially for small healthcare institutions that have limited spaces. Additionally, on-premise systems are prone to loss of information in case of fires and other catastrophic events that might damage the local servers that store the information [14]

## VII. IMPLICATIONS ON DATA SECURITY

There are multiple security challenges associated with institutional based EHR systems, although data stored in on-premise servers are less prone to outside interference and incidences of cyber-security. The fact that these systems are less prone to incidences of hacking does not imply that such events might not occur. In such situations, organizations might not have the capability to retrieve or restore the system from the hackers; this might lead to significant financial implications and loose of information. Additionally, the privacy and confidentiality of the patients might be compromised during such occurrences. Additionally, most organizations that operate institutional based EHR systems do not have backups for the data stored in their systems, or the backup is located within the facility. Information stored in such systems is vulnerable to environmental disasters or incidences, such as a fire, that are capable of causing damage to the infrastructure that houses the in-house servers. Such occurrences may lead to the loss of patient data and information.

## VIII. CLOUD-BASED ELECTRONIC HEALTH RECORD SYSTEM

On the other hand, cloud computing refers to a platform where the hardware and software are pooled together through a network that makes it possible to meet the system’s demands. Five characteristics are common with different cloud computing platforms. The first major, characteristic is on-demand self-service; this implies that system users can automatically access the system or get their demand met through the system without the need of any human interaction with the system administrators or IT personnel. Another common feature of a cloud computing platform is remote system access. The ability to access the system remotely implies that users can access any information from different parts of the world as long as they have enabling devices such as computers, and smartphones as well as an internet connection. Furthermore, the ability to simultaneously serve several users is another common feature of a cloud computing platform. Therefore, a cloud computing system has to have the ability to pool and redistribute resources according to the needs of the users. Most cloud-based systems are also known to be highly elastic; this implies that they can be changed or modified depending on the current needs and demands most cloud computing platforms also can track resource usage thus providing transparency for both the service providers and the consumers. Cloud-based systems can be classified into three major groups which include Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) [15]. Cloud-based systems can also be classified depending on the people who are meant to use them. For instance, private cloud systems are adopted and designed to serve the needs of private organizations. Such systems may either be managed by third parties or by the specific organization. On the other hand, public cloud systems can be accessed by the members of the community. These systems are similar to community cloud systems. Lastly, Hybrid cloud systems combine the features of organization and community systems in a single platform [15].

Recent reports regarding EHR systems indicate that most health care organizations are opting for cloud-based electronic health record systems compared to the traditional on-premise hosted systems [15]. The deployment environment for cloud-based systems is based on external serves that are located away from the user institution. Unlike the on-premise framework, the data stored on cloud-based servers can be accessed through the internet by multiple people in different parts of the world as long as they have authorized access or the passcodes that allow them to access the system. Though a cloud-based deployment environment has multiple advantages over the on-premise framework, there are also challenges associated with this framework.

## IX. BENEFITS OF A CLOUD EHR SYSTEM

Cloud-based systems have a wide variety of benefits compared to on-premise EHR platforms. Cloud systems have a high data storage capacity. Healthcare organizations produce a considerable amount of data daily. In this regard, organizations benefit significantly from systems that can store and process the information. Cloud EHR systems are easily scalable; this means that healthcare providers can adjust their network needs based on their needs and demands. Furthermore, cloud EHR systems also increase the ease of stakeholder collaboration and access to information [16]. The data stored in cloud servers can easily be accessed and retrieved through the internet [9]. Additionally, stakeholders and healthcare institutions can easily share medical information, thus easing the process of decision making and collaboration. Additionally, most cloud-based systems are incorporating Artificial intelligence and machine learning functionalities in their design. Such features reduce the amount of time required to process and to analyze medical information, thus ensuring that the extra time can be used to help patients.

## X. RISKS OF A CLOUD EHR SYSTEM

Cloud EHR systems are also associated with multiple disadvantages. To begin with, these systems are prone to information leaks, system downtimes, and improper handling of data by the service providers. Furthermore, all aspects and functionalities of cloud EHR systems are also required to comply with the Health Insurance Portability and Accountability Act (HIPAA) [17]. These functionalities may range from security and privacy protocols, among others. Ensuring HIPAA compliance can be a challenging task for most organizations and cloud service providers. Furthermore, organizations lose a significant level of system control in the case of cloud EHR systems. The system is controlled by third parties hence making the healthcare providers reliant on their services. Service providers who are reluctant to respond to system break downs or to maintain the network infrastructure may hamper hospital operations and services. Additionally, the cost of EHR systems significantly depends on t its features and capabilities. Organizations that require cloud EHR systems with sophisticated features may incur significant annual or monthly service subscription costs. Cloud EHR systems also need stable internet connections for them to operate efficiently. Poor connections may hinder the accessibility of information stored in the cloud. Additionally, one of the most significant concerns about cloud EHR systems is the issue of security. Data stored in cloud servers are prone to issues such as hacking, leakage, security breaches, and malware, among others. These issues may lead to the loss of information or cause patients' data to fall in the wrong hands which is a breach of patient privacy and confidentiality.

## XI. KEY DIFFERENCES THAT MAKE CLOUD-BASED EHR SYSTEMS TO BE MORE DESIRABLE THAN ON-PREMISE EHR SYSTEMS

They are multiple factors that distinguish cloud-based EHR systems from an on-premise platform. The first significant difference is in regards to customization and the ease of use. As stated before, organizations that rely on on-premise servers are responsible for maintaining and controlling all operations that pertain to the system. This implies that such organizations have to establish a team that is mandated to ensure the security and safety of the data as well as the frequent creation of backups to minimize the risk of information loss. Such a team has to have the ability to predict the space and organizational bandwidth requirement for both the present and the future to cater for organizational expansion. Furthermore, such teams have to have the knowledge and skills to handle any systems troubles or future upgrades by the software developers. On the other hand, cloud-based EHR systems do not require organizations to worry about maintenance and upgrading issues, and they can be customized more easily. This is because such duties are left in the hands of the cloud services providers, and thus, organizations do not need to employ full-time Information and Technology Personnel. Additionally, cloud-based systems are also more convenient compared to on-premise systems since the information stored in such servers can be accessed remotely from within and outside the institution. The ease of accessibility makes it possible for continuous and more and better-coordinated collaboration among medical care teams as compared to the on-premise EHR systems. The cloud-based systems also lead to more time savings and efficiency in service delivery compared to institutional-based systems since medical information can be accessed remotely; this not only benefits the physicians and care providers but also allows patients to receive timely access to care.

The cost of implementation of an on-premise based EHR system is also higher compared to that of a cloud-based system. Institutional based systems require organizations to bear the cost of installation, purchase of hardware and software, construction of a facility to house the servers as well as other supporting infrastructures. Organizations also need to hire a capable team of technicians and specialists to handle matters related to the system. Other costs that organizations might incur include the cost of maintenance and upgrading the system as well as the cost of acquiring a license and meeting all the legal requirements. These costs are incredibly high compared to the amount required to operate a cloud-based system where the service provider covers most of the costs.

## XII. OTENTIAL PRIVACY THREATS ASSOCIATED WITH CLOUD-BASED EHR SYSTEMS

As stated before, the data stored in cloud EHR systems are sensitive, and thus, it should not be exposed to third parties or other individuals who do not have the authorization to view the information. However, the issue of enhancing privacy remains to be a major challenge for organizations that operate cloud-based systems. Various threats threaten the privacy of information stored in cloud EHR systems. The greatest threat to the privacy of data and information is the issue of data theft, security breaches, as well as cases of hacking and physical attacks. According to a study conducted in the United Kingdom, increase in cases of cybercriminals targeting health data stored in cloud systems has raised a lot of concerns among patients in regards to how their information is stored or shared with third parties. Most of these crimes are committed with the aim of gaining financial benefits from such operations. The high value of the health information that is possessed by healthcare organizations makes the sector to be one of the most highly targeted by criminals. Present research indicates that medical information is now ten times more valuable than information from financial institutions [18]. The increased number of mobile devices and enhanced accessibility to the internet has also increased the privacy vulnerabilities of health information stored in cloud systems. Additionally, a report by the office of civil rights in the United States indicates that the healthcare sector was one of the most highly affected by cases of privacy breaches and leakages of patient-related information to the public as a result of inadequate privacy control measures.

Privacy threats in the healthcare industry can be divided into two main categories, which include contextual and content-oriented privacy. Contextual oriented privacy refers to the ability of third parties to access information regarding the patient’s sickness and health status. On the other hand, content-oriented privacy is a situation where healthcare organizations provide marketing agents and other third parties in regards to patients' health records without seeking the consent of the patient. Furthermore, HIPPA regulation mandates healthcare organization to ensure that patients can access and monitor how their health information is utilized. However, most organizations operate cloud-based systems have not been able to be fully compliant with this requirement of the HIPPA law [18]. The lack of patient involvement in the management of their health record increases the probability that the data might be exposed to privacy issues. Including patients in the management of their health records can reduce privacy issues.

## XIII. SECURITY THREATS IN CLOUD-BASED ELECTRONIC HEALTH RECORD SYSTEMS

As seen above, there multiple challenges that threaten the privacy of health information stored in the cloud. It is therefore crucial for organizations to put in place measures to protect this information from the above privacy challenges. Security threats in cloud-based systems may occur as result hardware, human factors, software related issues, and network factor and protocols. Human beings interact with the systems in most cases. It is, therefore, crucial to ensure that the people who interact with the system have an adequate understanding of its dynamics and operations. This reduces the chance that such people might engage in any activities that might compromise the security of the system. Additionally, the people who interact with the system should be well vetted to ensure that they are trustworthy and that they cannot engage in any unethical activities that might threaten the security or privacy of the information available in the system. Cloud service providers, as well as healthcare organizations, should adequately vet the people that interact with the system as a measure to reduce the security that human interaction poses to cloud EHR systems.

Hardware-level threats are among the riskiest since attacks at this level can lead to significant manipulation of data and the entire cloud system. Attacks at this level give an attacker enough power and flexibility to launch malicious commands. Attacks at the hardware level may occur undetected by malicious attacks detection protocols [19]. One of the most common strategies that are used to launch attacks at the hardware level includes the use of hardware Trojan. Hardware Trojans are launched through a deliberate modification to the system or its circuitry such that the system does not operate as it should operate. Hardware Trojans may alter the system in multiple ways. A hardware Trojan may be designed to negatively affect the error detection circuitry hence causing it to malfunction by accepting inputs that should otherwise be blocked. Trojans may also alter the system's power consumption rate, lead to incidences of service denial and exhaustion of system resources such as the internet bandwidth among others [20].

Furthermore, the increase in counterfeit goods has also led to an increase in the probability of attacks at the hardware level. Cloud service providers or organization either knowingly or unknowingly purchase substandard goods due to their low prices [21]. Such goods may be from untrusted suppliers, and they may end up containing hardware Trojans that might compromise the security of the system and the information stored within the servers. Additionally, there is also a possibility of side channel hardware attacks. Such attacks occur when people with malicious intentions gain information about the composition of the system from reading its electromagnetic radiations, electric consumption, among other approaches such as timing CPU or server operations [19]. Such information may be used to tamper with the system, thus leading to the leakage of sensitive system information. Multiple security measures can be used to handle potential security threats at the hardware level. One of the most common and effective approaches is the use of tamper-resistant hardware to reduce the risk of encountering attacks due to hardware Trojans as well as using hardware devices from trusted suppliers and manufacturers. Additionally, side channel hardware attacks can be minimized by putting in place measures to safeguard the physical information of the system such that attackers cannot aces or use this information to map out information from the system.

Additionally, the security of the cloud-based system can be compromised from the software level. The term software bug is used to refer to defect or flaws in a computer program [22]. Attackers can utilize such defects to gain access to the servers or the information in the system. A huge proportion of attacks arise from the exploitation of software bugs [23]. Such bugs can occur at the memory, input validation, or system access privileges functionality of the software that controls a cloud-based system. Attackers can take advantage of faulty memory functionalities to change the default data storage location of the system. Such an action can compromise both the safety and integrity of the information since data stored elsewhere apart from the systems default storage can be accessed by the attackers since it might not be protected by similar security protocols as the data stored in the default location. Additionally, changing the default storage location of the system may cause data to be stored in a different location that already has data stored within. Such an action may cause the system to overwrite on previously stored data hence compromising its integrity.

A cloud-based EHR record may also encounter security threats at the network infrastructure and protocol level. Unsecured network protocols make it easier for hackers and other attackers to gain access to the information stored in the system mainly by intercepting it during its transmission. Weakness in the network infrastructure mainly occurs as a result of system administrators and users who have insufficient knowledge in regards to the network infrastructure [24]. Attackers mainly exploit the Internet protocol address, the Transmission Control Protocol and the Domain Name System to infiltrate a cloud-based system at the software level. Attackers may impersonate a trusted system user, which allows them to access any information that was meant for the impersonated person. In this regard, the best and most common approach to prevent the occurrence of attack at the software level is the adoption of data encryption mechanisms [25]. Such mechanisms ensure that information and messages sent through the system can only be shared and viewed by the intended parties who have access to the decryption and security keys.

## XIV. CLOUD-BASED ELECTRONIC HEALTH RECORD SYSTEM.

Given the sensitive nature of medical information, health care providers, as well as cloud service providers, should partner to enhance the security and privacy is enhanced. This can be achieved by ensuring that the cloud EHR meets all the legal requirements. In the United States, the privacy and security of such digitized health records are regulated by HIPPA. The privacy rule by HIPPA regulates the accessibility of protected patient information [17]. The law argues that such information can only be retrieved through a court order or the patient's consent. HIPPA privacy laws also require entities that need to access protected patient information to seek consent from the patient and to use the least amount of information to meet their needs. Additionally, HIPPA requires digitized health records such as cloud EHR systems to meet several requirements as a measure to enhance security and privacy [17]. Moreover, the law also requires healthcare organizations to have training programs for workers dealing with patient's records as a measure to reduce the security and privacy risks associated with human factors. In this regard, training of workers and patients is also a viable option of reducing the security and privacy risks associated with cloud EHR systems. Moreover, sufficient planning on implementation of cloud-based EHR systems can play a crucial role in ensuring that organizations consider all the factors that may threaten the security and privacy of cloud EHR systems thus allowing them to take precautionary measures.

## XV. REQUIREMENTS THAT CLOUD EHR SYSTEMS SHOULD MEET TO MINIMIZE SECURITY RISKS

Cloud EHR systems should meet certain requirements to ensure that the information stored in them is secure. Some of these requirements include; authorized access. The information contained in cloud EHR systems is utilized and accessed by different people. In this regard, it is crucial to ensure that only the right people can access such data. Therefore, cloud EHR service providers should partner with organizations to establish identification credentials for all system users. Such a system can be achieved by providing all users with unique identification numbers and keys. Additionally, access to information should be role-based; this implies that different individuals who access the system have different information access levels based on their roles. A cloud EHR system should have the capability to guarantee high levels of privacy. This can be achieved through data encryption algorithms [26].

A cloud-based system should also have a mechanism for ensuring that patients approve or give their consent before any health information associated with them is retrieved or utilized by other system users or third parties. However, the system should also have the capability to avoid such restrictions during emergencies. Such functionality helps to uphold the privacy and confidentiality of patients' records. As stated before, different people can access the cloud EHR system. However, the system should have the capability to ensure that only relevant individuals can access certain types of information through access control measures. An ideal cloud EHR system should be capable of recognizing that although medical care providers are responsible for the information, the patients have a right to access the data. Additionally, cloud systems should also have features to guarantee and ensure the accuracy of the information; this can be ensured through functionalities such as change tracking [26]. Such a feature generates an alert when changes and modification are made to the data in the cloud servers. Such warnings are useful in enabling the system administrators to track the source of the change and to verify the authenticity of the information.

In addition to having the ability to guarantee the authenticity of the data, a cloud EHR platform should also have a feature that contains and noneditable register of all activities occurring within the system and their sources. The log should include activities such as logins, shared information, added information, deleted data, and any communication occurring within the system, among others. Such a feature ensures increases the ease of monitoring and tracking the activities of people who access the system, thus improving its security. Lastly, medical information requires to be maintained for an extended period to ensure continuity of care throughout an individual's lifetime. In this regard, a cloud-based EHR system should have the ability to archive a lot of information and make it available when the need arises. Data should be archived until a time when it is no longer required after which it can be deleted entirely from the system [26]

## XVI. MEASURES TO SAFEGUARD CLOUD EHR SYSTEMS

Given the fact that cloud EHR systems are prone to multiple security threats, it is crucial to put in place security measures to safeguard patient's health information from leakage, and interference from intruders and hackers among others. As stated before, different people can gain access to the cloud system. Such people include physicians, nurses, patients, and the employees of the cloud service providers. However, each of these users is different from the other regarding the type of information they require from the system. Therefore, it is not mandatory for all of the users to have access to all the data in the cloud system. Cloud service providers should map out the needs of all users and develop role-based access to information and system functionalities for each group of users [27]. The users can uniquely be identified using their assigned identification numbers. Such an approach will ensure those system users who fall under the doctor's category have access to all information and system functionalities. On the other hand, users who are classified under the maintenance personnel category can only access enough information to allow them to execute their maintenance operations effectively. Such limitations will reduce the risk of information leakage, and it will also enhance the privacy of the patients' data.

Implementing role-based access to the cloud EHR systems will protect the information from internal privacy and security risks. However, the most significant sources of security and privacy risks are external. It is, therefore, crucial to put in place protective mechanisms to safeguard the system from external attacks or incidences of a privacy breach. Cloud-based systems make it possible to access all information related to the patient through the internet hence increasing the number of people who can obtain such information. The larger the population, the higher the security risks. Cloud service providers and health institutions should take various measures to safeguard their networks from external interruptions. Network security can be enhanced through data encryption of all sensitive patient information [28].

Data encryption ensures that information can only be accessed and shared amongst the authorized people [28]. Furthermore, a digital signature can also be used to safeguard the authenticity and the integrity of information stored in cloud servers [29]. Digital signatures reduce the incidence of false data transactions by ensuring that reassuring users of the validity of the information. Additionally, digital signatures are unique; thus, they also make it possible to track the activities of all users who have access to the system. Cloud service providers should also ensure that they carefully and frequently monitor their networks as well as the activities of the users. Monitoring the systems makes it possible to quickly identify any unusual actions that might compromise the security of the system or disrupt normal operations and to take corrective measures. Track changes and activity logs are some of the features that can aid in monitoring the system as well as the activities [30].

## XVII. FACTORS THAT HEALTHCARE ORGANIZATION SHOULD CONSIDER BEFORE SELECTING A CLOUD SERVICE PROVIDER

From the above analysis, it is evident that the primary challenge facing an organization is ensuring the security and privacy of information that is stored in cloud HER systems. It is therefore essential to ensure that the selected cloud service provider can protect the data [31]. Organizations should begin by understanding what cloud storage entails as well as the services that are provided by the cloud service provider as well as the security mechanisms that are in place to ensure data privacy. Therefore, several factors should guide health institution in selecting a reliable service provider [31]. These factors include:

## XVIII. CERTIFICATION

Reliable cloud service providers should have the necessary certification to prove that they can provide the said services. Cloud service providers are required to comply with multiple third-party certification requirements as well as privacy laws. Possession of such documentation proves that the company can be trusted to protect an institution's health information.

## XIX. MONITORING

Additionally, organizations should also select cloud service providers that have the necessary cloud system monitoring tools in place. These tools should be automated and should be available for both the service provider and the clients. Additionally, the tools should have the capability to detect any changes or alterations made to the system and the data and to provide timely notifications that will allow the service providers or the organizations to take the necessary corrective measures to safeguard their data [32].

## XX. SUFFICIENT INFORMATION AND COMMUNICATION

Availability of information and prompt communication from the cloud service provider is a crucial aspect that organizations should consider before selecting a cloud service provider. Availability of information allows healthcare organizations to understand the activities of the cloud service provider as well as the measures and actions they are taking to safeguard the data stored in their servers [32]. Additionally, the availability of information and communication also implies that the cloud service provider can be relied upon in case of emergencies.

## XXI. EMPLOYEE LIFECYCLE

The data stored in EHR cloud systems are sensitive, and it should only be exposed to a few trusted people to avoid any leakages. Therefore, it is essential for cloud service providers to have a good employee policy that allows them to hire and retain competent and trustworthy workers. Additionally, cloud service providers should conduct thorough background checks on their employees before entrusting them with handling critical medical information. On the other hand, healthcare institutions that are seeking to adopt cloud EHR systems should examine the employee policy of potential cloud service provider to determine whether or not the employees can be trusted to safeguard the security and the privacy of the health information [32]

## XXII. THE PHYSICAL SECURITY

Health care institutions should also select cloud service providers who have secure physical facilities. The facilities that host the cloud servers should be adequately safeguarded with enough security protocol to prevent or minimize the risk of external intruders. Organizations that have secure physical facilities are more capable of guaranteeing the security and privacy of the information contained in the cloud servers [32].

## XXIII. ENVIRONMENTAL RISKS PROTECTION

Healthcare organizations should also select service providers that have put in place adequate measures to protect their servers from environmental activities such as fires and other calamities and their related damages [32]. Such actions help to minimize the risk of loss of medical information as a result of such occurrences.

## XXIV. BUSINESS CONTINUITY AND MANAGEMENT

Healthcare organizations should also select cloud service providers who portray sound management practices and appropriate business continuity models [32]. This will help to ensure that a change in management will not put a hospital's information at risk or cause the cloud service provider to fail.

### 3.3.3.8. BACKUPS

Medical care providers should also consider selecting cloud service providers who have adequate backup mechanisms to safeguard the stored health information from loss [32]. Back measures ensure that the information can be retrieved from different sources in case a failure occurs at one of the sources or if the data is compromised.

## XXV. APPROPRIATE SYSTEM DECOMMISSIONING APPROACH

Additionally, medical institutions should also select cloud service providers that have reliable decommissioning approaches. Decommissioning refers to the process of ending a partnership between two parties [32]. In this case, healthcare institutions should ensure that the decommissioning approach used by the cloud service provider guarantees that all previously stored data is completely removed from the servers at the end of the service tenure without any risk of data being copied by unauthorized users.

## XXVI. SUFFICIENT NETWORK SECURITY

The most crucial aspect that hospitals should consider before selecting a cloud service provider is the security mechanisms that have been put in place to ensure data privacy and security [32]. Reliable service providers should have strong tools for protecting their networks from intrusion or external attacks.

## XXVII. REDUCING SECURITY AND PRIVACY RISKS ASSOCIATED WITH CLOUD-BASED EHR SYSTEMS THROUGH SUFFICIENT CHANGE IMPLEMENTATION PLANNING

Adopting a cloud-based EHR is a technical process that needs to be carefully planned out to ensure a reduction in the risks associated with such a system. As discussed above, cloud EHR systems are prone to multiple security and privacy risks. These risk can be avoided through the system design and the features and by ensuring that the cloud service provider is reliable. However, adequate planning on the process of adopting a cloud EHR system can play a significant role in enabling organizations to identify the possible security and privacy loopholes and to take measures to ensure that they are sealed before the system is adopted. There are multiple change implementation models that organizations can use when moving from client-server EHR systems to a cloud bases system. Kotter's 8-steps approach towards change is one of the most effective methods that organizations can use to ensure that they cover all risks associated with moving patient records to the cloud [33]. The first step, according to this model, is to create the need and a sense of urgency for change. This step entails convincing stakeholders the importance of adopting a cloud EHR system as opposed to traditional health record systems. This step entails evaluating the threats and opportunities, engaging all stakeholders in discussions about the proposed change and seeking their support throughout the change implementation process. The next step, according to Kotter's model, is to form a strong coalition with all stakeholders and the changes leaders within the organization. The next step is to develop a vision for the change and to outline the values and develop the necessary strategies to achieve the desired change. The fourth step entails communicating the developed vision and addressing any uncertainties arising among stakeholders. Additionally, it is also crucial to identify any obstacles that might hinder the process of change implementation and to take measures to reduce the impact of such obstacles. Handling the obstacles empowers the change implementation team and enables the change process to move on as planned. Additionally, it is crucial to break down the change process into small achievable goals. Such a breakdown makes it easier makes it possible to evaluate wins and take the necessary measures to correct any arising obstacles. Moreover, it is easier to align the small tasks to the main goal as opposed to handling the whole project as one. After the change has been made, the next steps entail building on the change and integrating it into the organizational culture [33].

Based on this model, several key questions should guide an organization in deciding whether or not it is viable to adopt a cloud-based EHR system and in helping them to deal with the potential security and privacy challenges associated with cloud-based EHR systems. The first major question that an organization should consider before implementing a cloud EHR system is whether or not it is ready to adopt such a change. In this regard, the organization should consider the technological gaps, the financial implications, the human resource needs as well as the benefits and risks associated with adopting a cloud-based EHR system. The next step is to develop an effective project implementation team that will be capable of leading the process of adopting a cloud-based EHR system. Members of the lead implementation team should be obtained from all associated groups of stakeholders; this will ensure that the interests of all the members are represented and presented in the implementation process. Additionally, selecting individuals to represent each group of stakeholders will provide different perspectives in regards to the security and privacy risks from the points of view of all groups hence making it possible to address all the arising concerns and to minimize the occurrence of the identified risks [33]. Some of the core roles that should be considered when developing the project implementation team include the lead physician, the lead super-user, and the project manager. The function of the lead physician in the team is to act as a link between system users and the technical team. On the other hand, the lead superuser should be an individual with a lot of background information about the needs of an organization. This individual should be highly conversant with cloud-based EHR systems and procedures. Some of the core duties of such an individual include creating system templates in accordance with the needs of the organization, developing workflows, and coming up with standard operating procedures. Lastly, the project manager will play a significant role in acting as a link between the cloud service providers and the implementation teams and in managing the projects resources and deadlines [34].

After establishing the project team, the next step is to develop both the short term and the long term goals for adopting a cloud-based EHR system. The developed goals should be aligned to the organizational culture as well as to the rules and regulations that govern the process of care provision. Some of the major goals that an organization should prioritize include improvement of healthcare outcomes and processes, as well as enhancement of security and privacy of information stored in such systems. Having clearly developed goals and procedures will enable the project team to ensure that they work towards meeting them. Organizations also need to carefully analyze the available options in regards to the system vendors or cloud service providers. The choice of a cloud service provider should have a proven track record and the ability to meet the needs of the organization as well as the ability to ensure that information stored in the system is safe and secure.

Before, adopting a cloud-based EMR record, it is also crucial for organizations and the project implementation teams to ensure that they have sufficient understanding of the current systems and assets as well as the interaction between the different system devices and how they operate and work together. This understanding will play a crucial role in identifying the needed improvements and optimization measures that will make the cloud-based EHR records better compared to the current system as well as the extra actions that should be taken to enhance the security and privacy of the network as well as the health records. Healthcare organizations must also plan out on how to stay ahead to systems updates and maintenance. The ability of a cloud-based EHR system to remain secure and safe significantly relies on the level of maintenance and its ability to adapt to changes. Malicious third parties who might have intentions of hacking the system are continually developing new ways of beating the security measures that have been put in place to ensure the security and privacy of health records that are stored in cloud-based EHR systems [34].

Planning for system updates and maintenance ensures that organizations stay ahead of any security threats or any risks that might hinder the effectiveness and integrity of the system. Moreover, the privacy and security of health records may be compromised during the initial phase of moving the health records from the traditional platforms to a cloud-based system. In this regard, healthcare organizations should take plan on how to roll out the cloud-based EHR system. There are two ways through which a healthcare organization can launch a cloud-based system. The first method is referred to as the big bang approach. This method entails changing from a traditional health records system to the cloud-based system all at once. Though these methods may be fast, it is not convenient given the fact the organization may not have the full capability to handle such rapid changes, and errors and inefficiencies may have huge adverse effects on organizations and the healthcare delivery process. The alternative of the big bang approach is the incremental approach which entails adopting the cloud EHR in phases or one department at a time. However, this approach is slow compared to the big bang method. Nevertheless, it gives the organization enough time to make amendments and changes to elements that might compromise the effectiveness of the system and consequently, the security and the privacy of the health records. Therefore, sufficient change implementation planning is crucial for organizations that are planning to move from traditional health records systems to cloud-based EHR systems [34 ]. Adequate planning enables organizations to identify the potential implementation challenges as well as security and privacy risks that might be associated with cloud-based EHR systems, thus enabling them to take the appropriate measures to protect patients' records.

## XXVIII. REDUCING SECURITY AND PRIVACY RISKS ASSOCIATED WITH CLOUD-BASED EHR SYSTEMS THROUGH TRAINING OF EMPLOYEES AND PATIENTS

Most of the security and privacy risks that are linked with cloud-based EHR systems are either directly or indirectly associated with employees. In this regard, it is crucial to sensitize employees on their roles and the responsibilities toward upholding the privacy and security of the information stored in cloud-based EHR systems. As more healthcare organizations continually become reliant on cloud-based EHR systems, it becomes necessary to seek multiple solutions of enhancing the privacy and security of health records stored in such systems. Employee training programs should be a top priority for all healthcare organizations that integrate cloud-based EHR records in their operations. The training should be, and it should mainly focus on sensitizing the workers on the emerging cybersecurity issues. Research indicates that approximately 80% of individuals who are charged with controlling organizational cloud-based systems believe that the lack of awareness on cybersecurity issues is one of the greatest risks to the security and the privacy of information stored in such systems [34 ]. Additionally, insufficient information among workers also hinders the adoption of cloud-based EHR systems or any programs designed to enhance the security and privacy of health records [34 ]. Employee training is also backed by HIPPA regulations. The law requires all organizations that utilize cloud-based EHR records and other EHR systems to ensure the personnel who operate such systems are sufficiently supervised. Moreover, the law also requires healthcare organizations to ensure that there is the proper authorization of individuals or employees who are involved in handling EHR systems. All workers should be trained in security and privacy policies and procedures. Moreover, the law requires all organizations to ensure that they put in place the necessary sanction to impose against individuals who violate the outlined policies and procedures. An organization's training policy should be tailor-made depending on its human resource needs, given the fact that the needs differ from one organization to the other [34 ].

As mentioned before, the nature of cyber crimes and security threats that pose risks to cloud-based EHR systems evolves with time and technology, among other factors. It is due to this reason that cybersecurity training should be conducted frequently. Moreover, an organization should ensure that it reviews its subsequent training programs to ensure that it is aligned with emerging issues and challenges. The training should be conducted on a bi-annual or monthly basis to ensure that organizations leap maximum benefits from such a program. Training programs should combine different approaches, such as the use of newsletters, classroom-based courses, computer-based training, brochures, email alerts, and organized group discussions. It is also crucial for organizations to ensure that they document the training sessions on the topics handled, and the training materials utilized. Such documentation plays a crucial role in helping healthcare organizations to prove that they are compliant with HIPPA requirements during audits. The training of employees should occur at all levels of the organization. The training of employees allows them to understand how their actions can impact the security and the privacy of the information stored in the system [34 ]. Some of the concepts that employees need to to be taught is how to protect their passwords, the importance of using secure devices and networks while accessing the system, how to identify phishing attempts and avoid them, the measures to take in the event that they suspect that their system passwords have leaked or the system has been compromised as a result of their activities among others. Apart from training their employees, healthcare organizations should also ensure that they also conduct awareness and sensitization campaigns amongst their clients. The patients that are served by a healthcare organization that uses a cloud-based EHR system also play a crucial role in enhancing the security and privacy of their information. Therefore, healthcare organizations should also ensure that they educate them on how their actions influence the security of their medical information. The patients or clients should also be trained on how to protect their passwords, the importance of using secure devices and networks while accessing the system, and how to avoid phishing traps and malware that might compromise the security and privacy of patients' records that are stored in cloud EHR systems. Through the training of workers, organizations can minimize the risk to security and privacy of health records, that are stored in cloud-based EHR systems, that is associated with the human element of all healthcare organizations

## XXIX. DISCUSSION OF FINDINGS

EHR systems fall under two main categories, namely; client-server and cloud-based EHR [7]. In the client-server system, information is stored in servers and systems that are controlled by the specific institution that utilizes the platform. On the other hand, cloud-based systems store data in external servers and are controlled by third-party institutions [8]. The deployment environment of a cloud EHR determines whether or not it can be classified as Cloud-Based or On-premise. Each of these systems has unique advantages and disadvantages. However, organizations prefer cloud EHR systems as a result of the advantages that it has over an on-premise system. Such advantages include high data storage capacity, system scalability, ease of stakeholder collaboration and access to information, and low maintenance cost. However, there has been an increase in concerns among stakeholders in the healthcare sector in regards to the security and privacy of information stored in cloud servers hosted by third-party organizations. These systems are prone Data stored in cloud servers are prone to issues such as hacking, leakage, security breaches, and malware, among others. These issues may lead to the loss of information or cause patients' information to fall in the wrong hands which are a breach of patient privacy and confidentiality to information leaks, system downtimes and improper handling of data by the service providers. The high value of the health information that is possessed by healthcare organizations makes the sector to be one of the most highly targeted by criminals. Present research indicates that medical information is now ten times more valuable than information from financial institutions.

Privacy threats in the healthcare industry can be divided into two main categories, which include contextual and content-oriented privacy. Contextual oriented privacy refers to the ability of third parties to access information regarding the patient's sickness and health status. On the other hand, content-oriented privacy is a situation where healthcare organizations provide marketing agents and other third parties in regards to patients' health records without seeking the consent of the patient. The security and privacy of cloud electronic health record systems may be compromised at the hardware level, software level, and the internet infrastructure and protocols level. Cloud service providers should, therefore, be capable of identifying the potential source of risks and putting in place measure to protect the information stored in their servers from any of the above security risks

Some of the security measures that healthcare organizations, as well as cloud service providers, should ensure are present in a cloud-based electronic health record system include; role-based and authorized access to information and system functionalities. Implementing role-based access to the cloud EHR systems will protect the information from being accessed by unauthorized people. However, the most significant sources of security and privacy risks are external. Cloud service providers and health institutions should take various measures to safeguard their networks from external interruptions. Network security can be enhanced through data encryption of all sensitive patient information [28]. Moreover, cloud service providers should integrate data encryption systems in the cloud servers Data encryption ensures that information can only be accessed and shared amongst the authorized people [28]

Furthermore, a digital signature can also be used to safeguard the authenticity and the integrity of information stored in cloud servers [29]. Digital signatures are unique; thus, they also make it possible to track the activities of all users who have access to the system. Moreover, the integration of Track changes and activity logs features can aid in monitoring the system as well as the activities, thus enhancing security and privacy [30]. Organizations should ensure that they select reliable cloud service providers who meet all the certification and legal requirement to offer such services. Implementing these measures will reduce the security and privacy risks associated with cloud-based electronic health records systems hence enhancing the privacy and confidentiality of patient information. Lastly, hospitals can likewise limit the security hazards related with moving patients' records to the cloud through cautiously arranging out the implementation procedure of the framework and putting into thought every one of the elements that may have an impact on the security and the privacy of the information stored in cloud servers. Furthermore, adequate preparing and training of workers and patients in regards to the security of a cloud EHR framework is also an important risk reduction measure. Preparing these partners on how their activities impact the security of the framework, and the measures they should take to improve the wellbeing of data stored in cloud-based EHR frameworks is additionally a practical methodology towards decreasing the security and privacy risks.

## XXX. CONCLUSION

Conclusively, health organizations are increasingly adopting electronic health record systems. The main reason behind the widespread adoption of EHR systems is to promote timely access to patient records and information as well as to improve efficiency and effectiveness in the care delivery process. Some of the advantages of these systems include a reduction in medical diagnostic errors, ease of access to medical information, a decrease in other medical errors such as providing wrong prescriptions to patients. Additionally, EHR systems also promote collaboration among various medical stakeholders, thus improving decision making and consequently, healthcare delivery. However, these systems are also associated with multiple cons, such as an increase in the risk in the occurrence of medical malpractice claims. Cases of malpractice are more common during the initial stages of EHR adoption and implementation.

Apart from increasing the likelihood of the occurrence of medical malpractice claims, EHR systems also influence the outcomes of such litigation. As opposed to traditional health record systems, EHR systems can easily provide information that may be used to either hurt or support a medical malpractice case. Furthermore, some EHR systems provide medical suggestions to medics and aid them in decision making. However, the actions taken by physicians or any decisions made are ultimately their liability. In this regard, EHR systems are also likely to increase the occurrence of errors in the healthcare provision process. Some of the common errors include prescription error and dosage errors. EHR systems fall under to main categories, namely; client-server and cloud-based EHR. Each of these kinds of systems has unique pros and cons. However, most organization are increasingly adopting cloud EHR systems due to the multiple advantages that these systems have over the on-premise based systems. However, there are multiple risks associated with cloud-based platforms, mainly in relation to security and privacy. The security vulnerabilities can occur at the hardware, personnel, software and network infrastructures and protocol levels. It is, therefore, crucial for healthcare organizations as well as cloud service providers to ensure that their systems meet specific minimum requirements and that they have adequate security mechanism measures in place, such as authorized and role-based access to the system, data encryption, and frequent system monitoring through track changes and digital trails. Furthermore, organizations should consider multiple factors before selecting a cloud service provider; this will ensure the selected service provider is reliable and they can be trusted to ensure the security and the privacy of the information stored in their servers. Healthcare organizations can also minimize the security risk associated with moving patients' records to the cloud through carefully planning out the implementation process of the system and putting into consideration all the factors that might increase the privacy and security risk associated with cloud EHR systems. Additionally, sufficient training of employees and patients that have access to the system can also play a crucial role in enhancing the privacy and security of a cloud EHR system. Training these stakeholders on how their actions influence the security of the system and the measures they should take to enhance the safety of information stored in cloud-based EHR systems is also a viable approach towards reducing the security and the risks privacy. Conclusively, putting all these factors into consideration will minimize the security and privacy risks associated with cloud EHR systems, thus helping healthcare institutions to safeguard their patients' records.

## XXXI. REFERENCE

[1] Pattinson, H. (2011). *E-Novation for Competitive Advantage in Collaborative Globalization: Technologies for Emerging E-Business Strategies: Technologies for Emerging E-Business Strategies*. Hershey, PA: IGI Global.

[2] Fasano, P. (2013). *Transforming Health Care: The Financial Impact of Technology, Electronic Tools, and Data Mining*. Hoboken, NJ: John Wiley & Sons

[3] Almunawar, M. N., Anshari, M., Younis, M. Z., & Kisa, A. (2015). Electronic Health Object. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 52,* 004695801561866. doi:10.1177/0046958015618665

[4] Snipes, C. (2016). The Use of the Electronic Health Record in Behavioral Health Quality Improvement Initiatives. *Quality Improvement in Behavioral Health*, 193-206. doi:10.1007/978-3-319-26209-3_13

[5] Treas, L. S., & Wilkinson, J. M. (2013). *Basic Nursing: Concepts, Skills, & Reasoning*. Philadelphia, PA: F.A. Davis.

[6 ] Gamble, Molly. "5 Legal Issues Surrounding Electronic Medical Records." Becker's Hospital Review. Last modified 2012. https://www.beckershospitalreview.com/legal-regulatory-issues/5-legal-issues-surrounding-electronic-medical-records.html.

[7] Kelley, T. (2016). *Electronic Health Records for Quality Nursing and Health Care*. DEStech Publications.

[8] Becchetti, C., & Neri, A. (2013). *Medical Instrument Design and Development: From Requirements to Market Placements*. Hoboken, NJ: John Wiley & Sons.

[9] Singh, M., Gupta, P., Tyagi, V., Sharma, A., Ören, T., & Grosky, W. (2017). *Advances in Computing and Data Sciences: First International Conference, ICACDS 2016, Ghaziabad, India, November 11-12, 2016, Revised Selected Papers*. Basingstoke, England: Springer.

[10] Blum, B. I. (2012). *Clinical Information Systems*. Berlin, Germany: Springer Science & Business Media.

[11] Wenjia Li, Voris, J., & Artan, N. S. (n.d.). Security, trust, and privacy for cloud computing in Transportation Cyber-Physical Systems. *Data Security in Cloud Computing*, 171-195. doi:10.1049/pbse007e_ch8

[12] Lamar, M. (2011). EHRs in the cloud: contract protection for a rainy day. J AHIMA, 82(7), 48-49.

[13] Levy, A. (2016). *Healthcare and Technology Today: A Guide for Providers and Practice Managers*. Morrisville, NC: Lulu.com.

[14 ] Wager, K. A., Lee, F. W., & Glaser, J. P. (2013). Health Care Information Systems: A Practical Approach for Health Care Management. Hoboken, NJ: John Wiley & Sons.

[15] Patel, Sheel. "Challenges of Migrating EHR Systems to Cloud." *Undergraduate Research Journal* 16 (2016). Accessed May 26, 2019. https://scholarworks.iu.edu/journals/index.php/iusburj/article/view/22183.

[16] Pradhan, C., Das, H., Naik, B., & Dey, N. (2018). *Handbook of Research on Information Security in Biomedical Signal Processing*. Hershey, PA: IGI Global.

[17] Hoffman, S. (2016). *Electronic Health Records and Medical Big Data: Law and Policy*. Cambridge, England: Cambridge University Press.

[18] Riordan, F., Papoutsi, C., Reed, J. E., Marston, C., Bell, D., & Majeed, A. (2015). Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. *International Journal of Medical Informatics*, *84*(4), 237-247. doi: 10.1016/j.ijmedinf.2015.01.008

[19] Li, Q., GAO, H., Xu, B., & Jiao, Z. (2008). Hardware Threat: The Challenge of Information Security. *2008 International Symposium on Computer Science and Computational Technology*. doi:10.1109/iscsct.2008.217

[20] Chakraborty, R. S., Narasimhan, S., & Bhunia, S. (2009). Hardware Trojan: Threats and emerging solutions. *2009 IEEE International High-Level Design Validation and Test Workshop*. doi:10.1109/hldvt.2009.5340158

[21] Karri, R., Rajendran, J., Rosenfeld, K., & Tehranipoor, M. (2010). Trustworthy Hardware: Identifying and Classifying Hardware Trojans. *Computer*, *43*(10), 39-46. doi:10.1109/mc.2010.299

[22] Shahriar, H., & Zulkernine, M. (2012). Mitigating program security vulnerabilities. ACM Computing Surveys, 44(3), 1-46. doi:10.1145/2187671.2187673

[23] Liu, S., & Cheng, B. (2009). Cyber attacks: Why, What, Who, and How. *IT Professional*, *11*(3), 14-21. doi:10.1109/mitp.2009.46

[24] Cole, E., Krutz, R. L., & Conley, J. (2005). *Network Security Bible*. Hoboken, NJ: John Wiley & Sons.

[25] Rass, S., & Slamanig, D. (2013). *Cryptography for Security and Privacy in Cloud Computing*. Artech House.

[26] Alabdulatif, A., Khalil, I., & Mai, V. (2013). Protection of electronic health records (EHRs) in the cloud. *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. doi:10.1109/embc.2013.6610469

[27] Kim, D., & Solomon, M. G. (2013). *Fundamentals of Information Systems Security*. Burlington, MA: Jones & Bartlett Publishers.

[28] Nemati, H. (2010). *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering: Information Encryption and Cyphering*. Hershey, PA: IGI Global.

[29] Management Association; Information Resources. (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global.

[30] Cambron, G. K. (2012). *Global Networks: Engineering, Operations, and Design*. Hoboken, NJ: John Wiley & Sons.

[31] Gasch, A., & Gasch, B. (2010). *Successfully Choosing Your EMR: 15 Crucial Decisions*. Hoboken, NJ: John Wiley & Sons.

[32] JPC Rodrigues, J., De la Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. *Journal of Medical Internet Research*, *15*(8), e186. doi:10.2196/jmir.2494

[33] Pollack, Julien, and Rachel Pollack. "Using Kotter's Eight-Stage Process to Manage an Organizational Change Program: Presentation and Practice." *Systemic Practice and Action Research* 28, no. 1 (2014), 51-66. doi:10.1007/s11213-014-9317-0.

[34] "Electronic Health Record (EHR) Implementation Guide." Continuum. Last modified July 27, 2018. https://www.carecloud.com/continuum/electronic-health-record-ehr-implementation-guide/.