JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBERSECURITY PROTOCOLS FOR ELECTRONIC HEALTH RECORDS (EHRS): BEST PRACTICES FOR PROTECTING SENSITIVE PATIENT DATA IN EHRS FROM CYBER ATTACKS

VENKATESWARANAIDU KOLLURI

Sr. Data Scientist, Department of Information Technology

***ABSTRACT*—The aim of this paper is to explore the various opportunities to create affordable, efficient, and effective security protocols for electronic health records (EHRs). The increased adoption of EHR systems offers many advantages for health organizations and patients. These potential benefits are tempered by anxiety over various security and privacy issues. The privacy of sensitive health information is a key issue for patients and their willingness to adopt EHRs [1]. The very future of EHR success may depend on the public's sense of security. There are many standards and best practice documents available for EHR security guidelines, but many organizations have found them to be too numerous, too complex, and not directly actionable. Our goal is to address a security protocol in terms of an ontology of directly actionable security processes that will protect the most sensitive EHR information. These processes would be used to automatically monitor the flow of patient information and detect any violations of privacy policies. This detection will immediately trigger a corrective action to resolve the policy violation [1,2]. The need for directly actionable security processes signifies that we will use EHR system data as a basis to force changes in behaviors that directly affect the security of patient information. We will avoid creating security policies that are broad, too abstract, or not directly enforceable within an EHR system. Primarily, our work targets the security of patient information that is mental health or behavior related; implication of released information could be detrimental for future employment or insurance opportunities. This area of security has received little attention in comparison to the security of general patient information.**

***Keywords*— E-health, electronic health record, health informatics, health services, computer security, data protection, information security, confidentiality, privacy, computer crime, data security policies, security management, medical records system, user authentication, cryptography, firewall, intrusion detection, antivirus agents, security evaluation, ISO, standards, legislation, regulation, Health Insurance Portability and Accountability Act, General Medical Council, Caldicott guardians, patients.**

I. INTRODUCTION

Data protection has received a lot of attention amidst rapid use of digital technology in the health sector. Cybersecurity protocols are of significant importance, being the last defense against cyber attackers trying to gain access to confidential patient data. With a huge amount of data including complete medical histories, diagnostic information and treatment plans, EHRs become the ultimate target for malicious actors seeking to take advantage of security flaws[2]. Thus, adherence to the standard cybersecurity principles is necessary to protect the integrity, confidentiality, and availability of EHRs, which enables the patients and healthcare workers to feel secure and consequently physically safe.

Among the critical challenges associated with securing EHRs is their involvement in a diverse ecosystem of parties that are behind creating, maintaining, and granting access to them. Healthcare workers, IT personnel managing systems, as well as the external vendors rolling out software solutions provide an expansive network, which in turn, makes numerous potential entry points for the cyber threats [2,3]. As a result, a security framework should feature not only the technical measures but also strong policies, training programs and routine audits addressing in entirety every part of the operations system. Healthcare information security awareness and responsibility development helps strengthen healthcare systems against cyber-attacks and to successfully handle both existing and future threats.

Implementation of the encryption, authentication, and access control mechanisms are among the central elements of the cybersecurity protocols for the EHRs as an effort to enforce the strict data protection measures. Encryption algorithms help to keep an EHR that contains unreadable data from the unauthorized users, thus prohibiting even after a breach it could still maintain confidentiality [3]. Additionally, multi-factor authentication protocols add an extra security layer by requiring multiple credentials for authentication, e.g. passwords, biometrics, or security tokens. Hence, combining identity and access management with role-based access controls, which are designed to limit user privileges centered on their individual roles and responsibilities, helps in the prevention of unauthorized access.

EHR systems require new skills and new attitudes on the part of clinical providers. This can create great difficulties, at least in the short term. For example, a study of physician satisfaction with an EHR system at an academic medical center revealed that most physicians were dissatisfied with the system, in large part due to insufficient training in its use[3]. Another common physician complaint is that EHR systems are an impediment to patient communication. Because of these and other issues, physicians and other clinical providers may resist using EHR systems if not compelled to do so. Users' negative attitudes and low skill level can, in turn, impede the successful implementation of the EHR system. Failure to achieve

widespread user acceptance is a chief reason for the failure of EHR systems. Another study of an integrated EHR system spanning several healthcare delivery organizations found that the initiative had to be abandoned because significant portions of it were never used. EHR systems have also been criticized for their effects on physician workflow[4]. One study found that physicians tended to spend more time on computer tasks and less time with patients after the implementation of an EHR system. EHRs have complex effects on workflow and can impede efficiency if the system is not well designed. Finally, EHRs carry some increased risks to information integrity. An analysis of a system for computerized prescription ordering found that the rate of medication error increased significantly after the new system was installed. This was because there was incompatibility between the system and the process - lack of flexibility in the system's design. The error rate finally dropped to the baseline after the new system was discontinued. These errors will happen generally in any EHR implementation.

EHRs have enabled physicians to access patients records remotely and to exchange medical data among themselves. This feature allows diversification of patient care and cost saving by avoiding repetition of services. The EHR systems are useful to clinical researchers with regards to large scale studies of different treatments. EHRs help to determine which treatments are the most effective by examining patterns of care. These systems also make it possible to assess the cost-effectiveness of various treatments. EHRs also give a boost to the quality of care rendering medical information available to all of those that provide medical care, including nurses [5]. Lastly, EHRs can assist to automate and streamline the clinician's workflow. For example, EHRs get rid of the need to manual the same data in a patient's chart over and over again. As a result, the probability of misspelling due to illegible handwriting considerably decreases.

II. RESEARCH PROBLEM

The main research issue in my paper is to identify and evaluate the most effective cybersecurity habits and practices for the Electronic Health Records (EHRs) protection against cyber-attacks. This involves a detailed assessment of cybersecurity frameworks, encryption methods, authentication mechanisms, access control policies, and risk assessment approaches that are specially designed for the healthcare sector. The study will tackle the multi-faceted issues intrinsic to secure EHR, including the many actors involved, the dynamic cyber threats, the HIPAA compliance constraints and the scope as well as the integration with the medical professionals to run EHR systems[6]. There is an overall lack of knowledge about what the law required, which led to unnecessarily restrictive conditions on the release of records. Currently, there lacks a standard protocol to enforce security and privacy measures for EHRs. The healthcare providers unaware of the deviations from HIPAA all cited privacy and confidentiality concerns as the reasons for not disclosing the medical records. Current practices for releasing the medical records have violated patient autonomy and HIPAA, as the healthcare providers have based their decisions on added restrictions of the law to prevent information disclosure and online searches [7]. An example of this would be a study on a child's hospitalization at Montefiore Medical Center where, despite 6 consents to information release by the child's mother, records were still not disclosed to researchers due to confusion on the extent of consent for future research.Though standards such as the Health Insurance Portability and Accountability Act (HIPAA) provide regulatory guidelines on security and privacy, the implementation and enforcement of these recommendations rely on the health organization. Current literature has suggested that the recommendations set forth from HIPAA are often too vague and broad to be effectively implemented into a security system for EHRs [1]. Although the Department of Health and Human Services has begun to implement this with audits in 2012 to evaluate HIPAA security rule compliance [7]. The rules set forth in HIPAA do not anticipate changes in technology and the current environment of healthcare delivery, as seen with private physicians and researchers who are not familiar with the complex law and its implications on their practices. These sets of individuals are less likely to have the knowledge or resources to effectively translate HIPAA to protocols for EHR security. Failure to understand HIPAA has resulted in unintentional violations of patient privacy and confidentiality by the healthcare providers.

III. LITERATURE REVIEW

A. EHR SECURITY

Common security incidents and a lack of awareness have led to a generally negative perception of EHR security, which is reflected in another study that examined patient and provider attitudes to the privacy and confidentiality of EHRs and health information exchange in primary care [7]. Failure to address the concerns of both these groups regarding security and privacy of EHRs can hinder the progress of utilizing EHRs and prevent potential benefits to patient care. High-quality EHR security is necessary to change this negative perception and enable patients and providers to have confidence in EHR use.

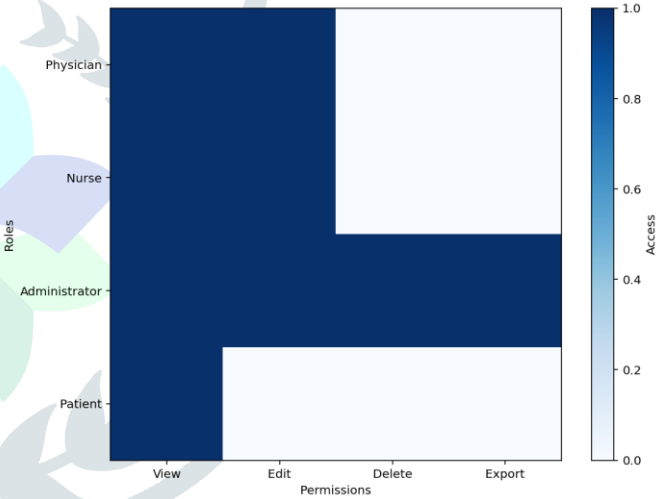

Fig. 1 Access Control Matrix for EHR Systems

Five studies highlighting the clinical consequences of security incidents and the need for improved security for EHRs were reviewed [8]. These incidents ranged from minor to serious in nature and involved both internal and external sources. Results have shown that often patients are completely unaware that security breaches have compromised their data. This illustrates the potential for adverse patient outcomes resulting from unauthorized access to EHRs is not immediately identifiable.

This section will highlight the importance of EHR cybersecurity and review literature currently available. In healthcare, as previously mentioned, EHRs are important in maintaining patient health and providing necessary information to healthcare professionals. Without proper security protocols in place, patient safety may be jeopardized. Cybersecurity of EHRs is necessary to protect medical data from unauthorized access, use, disclosure, disruption, modification, or destruction [8,9]. By ensuring the data is kept safe, it maintains the privacy and trust of patients and prevents any negative impact on their health and safety. When data is both accurate and secure, its quality makes a contribution to the overall health and well-being of our society and to future healthcare of individuals. It also aims to aid healthcare management, public health, and

reducing healthcare costs [1]. Because the impact of EHRs is both personal and widespread, it is important to recognize the significance of maintaining patient data security. Cyberattacks can harm EHR availability and integrity, thus increasing the potential damage to patient safety.

B. Importance of Cybersecurity in EHRs

The importance of cybersecurity in EHRs has always been a significant topic of discussion. Many attempts have been made by experts to prevent EHRs from being exposed to the many different threats of cybersecurity. Cybersecurity is important to the EHR for a number of reasons [10]. Records often contain sensitive information, which has to be protected according to the laws in many communities. Hacking into a medical record system can be very profitable. If the data is not protected, it can be easily exploited when it is transferred over public networks. Often, the storage of backups and the duration data is stored is not taken into account with many EHR systems. However, when considering the legal requirements of keeping medical records, data can be retained for many years in which it has to be ensured that the integrity of the data is maintained, and the records are kept available as and when required. An example of the consequences from this was an incident in Greece, where it was found that individuals were able to access and view the medical records of the then Prime Minister Kostas Karamanlis [10]. This had been done by using the simplest method of hacking, where the attackers had used the login names and passwords of authorized users to gain access into the system. This simple security breach was a major embarrassment to the government as the hospital involved was a state hospital. This could have been easily prevented if the system had proper security protocols enforced to prevent unauthorized access to the records. This strongly illustrates the sensitive nature of the private data contained in EHRs. EHR systems are one of the most security-critical information systems to exist in today's society.

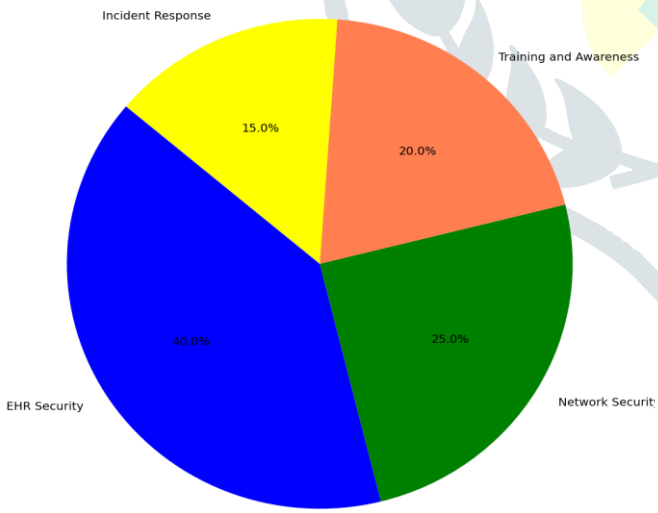

Fig. 2 Proportion of Cybersecurity solutions for EHRs

C. Common Cybersecurity Threats in EHRs

Multiple studies have outlined the vast array of potential cybersecurity threats prevalent to EHRs. One prominent study conducted by the California Healthcare Foundation identified the following key EHR threats: unintentional data disclosure, unauthorized data access, and data integrity loss. EHR Security breaches include employees or outside parties viewing and/or altering data without authorization and a loss of data integrity. It is important to understand the array of threats which can compromise EHRs in order to best recognize which security protocols are in need and will be most effective [11]. This understanding will also aid in the prevention of medical identity theft and will ultimately maintain the integrity of the healthcare system. It has been emphasized that the range of EHR threats are constantly evolving dependent on the advancing technology and will subsequently require ongoing modifications to security protocols. A government report on cybersecurity in health care states that as the use of EHRs become more widespread, hackers are increasingly targeting the health care sector with higher frequency and intensity. This suggests that current security measures are not sufficient in protecting EHRs and as mentioned in the title of the government report, there is a need to move beyond the baseline in cybersecurity readiness [12]. Capturing the scope of this issue, it has been noted that EHR security is usually an afterthought for people designing the systems and applications, software developers are more focused on building applications that meet the needs of hospitals and physician using and EHRs are built to be more accessible, so security measures can often be missed in the design phase. This current focus will result in increased vulnerability of EHRs and further emphasize the importance of recognizing and initiating improved security protocols.

D. Current Cybersecurity Protocols for EHRs

The primary protocol for much of the patient data that existed pre-EHR involves regulations outlined in the Health Insurance Portability and Accountability Act (HIPAA)[13]. HIPAA has made strides toward improving the privacy and security of patient data through the introduction of the Privacy Rule and the Security Rule. On the other hand, HIPAA has been brought into discussion for its being too open-ended sometimes, such that organizations have varied interpretations about what actually constitute security measures [14]. The provision of the Security Rule has often been challenged due the fact that it lacked the focus areas which were relevant to EHRs, such as authentication of electronic protected health information and provisions for its long-term preservation. On the contrary, researchers have been finding that these criticisms led to the development of specific protocols.In the past year or so, both public and private sectors conducted a lot of research on cybersecurity, a data protection standard that protects the privacy of personal information and regulates unauthorized access. Nonetheless, the main concern has targeted protecting the patients' data in general rather than setting specific rules for EHRs. This is as a result of the fact that EHRs are still evolving technologies and they are yet to be generally adopted as recent as 15 years ago[14,15]. As such, a large part of the protocols and infrastructure concerning the safety of EHRs has been accepted from the universal standards for data protection of a patient. These disparities though have been noticed by researchers and policy makers, and more specific protocols have in fact been developed to help ensure EHRs are secured.

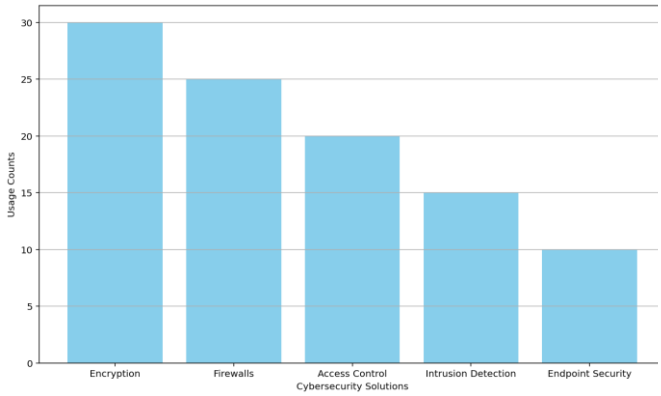

Fig. 3 Distribution of EHR Cybersecurity best practices

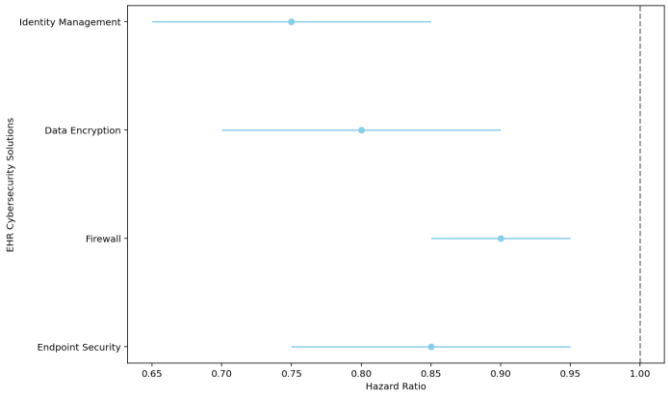

Fig. 4 Impact of EHR Cybersecurity Solutions

E. Challenges in Implementing Cybersecurity Protocols for EHRs

There are numerous challenges to implementing cybersecurity protocols for EHRs. One of the primary reasons that cyber threats to EHRs are so successful is the lack of a centralized security model. Traditionally, security has been perimeter-based, meaning anything inside the network is implicitly trusted. This model is completely ineffective for EHR security, as EHRs are meant to be shared among many different parties in many locations. Implementing a more effective security model will be difficult due to the large number of different EHR systems and vendors that currently exist[15,16]. In order to share information security credentials among systems, the systems must have some form of common identity and be able to validate the authority of the other systems and users. Developing a common identity between different systems will be a difficult task in itself and could likely require significant changes to the systems already in place. These changes will be time-consuming and often costly, meaning there is little incentive for EHR vendors to voluntarily make them. Without a significant change in the incentive structure, it is unlikely that the central security model needed for EHR security will ever become a widespread reality.

F. Best Practices for Cybersecurity in EHRs

Originally published in 2014 and led by Dr. Mohammed Almalag, this article has been created to offer the user an insight into the best practices of cyber security in EHRs. Even though this article is 5 years old, a lot of the information is still relevant. This is due to the health industry and its systems not having much change and can be viewed as both a positive and negative. Dr. Almalag says that it is positive because not much change offers continuity in care and avoiding medical error through event files[17]. However, the negative side to this is that if a hacker were to gain access to an event file, the information could be altered and the results could be damaging to the patient. Therefore, it is essential to ensure that EHR systems are securely practiced in prevention of unauthorized change, whilst keeping focused on the potential risks that it could cause to the patients[17,18].

G. Emerging Trends in EHR Cybersecurity

Medical data is worth a lot of money on the black market due to the fact that cyber security is weak. In 2016, healthcare was the industry with the most cyber attacks. Over 88% of all attacks on social industries were on healthcare [1]. New Residency for Cyber security and Health Technology. With the newly found importance of cyber security in healthcare, it has sparked not only programmes and courses, but specifically a residency. One residency that is available, sponsored by the Agency for Healthcare Research and Quality (AHRQ), aims to increase the knowledge and experience in health informatics and cyber security. The duration of the residency is for 2 years. AHRQ is dedicated to improving the safety and high quality of American healthcare by the means of research and evidence-based methods [18]. The aim of this residency directly reflects the importance of cyber security in healthcare – by having more knowledgeable workers, it can decrease any possible threat to patient information. This could set up for great advancement in the future for cyber security in healthcare; if knowledge and awareness are increased, there may be improved infrastructure with superior protocols and protection. This is only the beginning of advanced cyber security in healthcare but is a very positive sign for the future [1]. An increased focus on the development of new and efficient software and hardware for record keeping aims to improve the presence and effectiveness of cyber security. This is due to many of the present systems having security flaws and are easily susceptible to attack. By having secure systems, it is possible to reduce the prevalence of data breaches and provide a safe environment for patient information [18]. This is an ongoing process, and developments of more secure systems will be continuous as threats to cyber security are constantly evolving. This is a long-term goal to solidify safety and protection of patient information. Identifying and preventing attacks early on is a much better approach rather than dealing with the consequences.

IV. SIGNIFICANCE AND BENEFITS

As national health organizations begin to implement the suggested cybersecurity measures and technology which would safeguard EHRs, their action will contribute immensely to the American economy. The US Economy is believed to lose from $69 billion to $318 billion yearly from data theft. Implementing security measures that prevents EHR from being stolen is a healthcare organizations contribution to decreasing the total amount of data theft in the US, which in turn results in huge cost savings for the US economy [18,19]. Besides data theft, application downtime, which in case of EHRs can be the result of security breaches that cost US economy approximately 8 billion dollars yearly is also an additional problem. However, a secure environment for EHRs will prevent system damage and also save the American economy several billions of dollars every year by eliminating system breakdowns. A survey conducted in 2005 estimated that the frequency of computer security incidents in the US cost businesses and other

organizations $67.2 billion per annum. The result of more computerization of health records, therefore, could be an expected amount of security related to EHRs among the projected $67.2 billion of this amount[19]. Through elimination of security incidents by EHRs, healthcare providers can save tens of billions of dollars. Therefore, it would be reasonable to expect that cybersecurity prevention would save the US economy at least $100 billion over the next decade. With the growing national debt and increasing global economic competition, it is imperative that the US finds ways to cut costs and increase efficiency in public and private sectors. A total savings of $100 billion or more resulting from cybersecurity prevention with EHRs would be a significant contribution towards achieving that goal [19,20].

V. FUTURE

With the rapid increase of machine learning and AI in the healthcare sector, there will be a greater need for the protection of patient data. While these technologies may aid in many medical breakthroughs, it creates an avenue in which a cyber-attacker can alter or destroy data. EHR systems must be prepared for this potential threat. An opportune way to change this would be strict government enforcement of cybersecurity measures in healthcare. This would create a more level playing field since all organizations would be held to the same standard and it can reduce the risk of cyber-attacks being targeted to smaller organizations who may have weaker security. This would, however, require the government to allocate a substantial amount of resources toward the protection of EHRs [20]. With today's political standing of healthcare in the U.S., it is uncertain when or if such efforts will take place.

The most efficient way to protect against intrusion is a consortium of healthcare organizations sharing intelligence and best practices on cyber-defense. Though this idea is favorably a realistic approach, at this current time the U.S. lacks the governance and incentive to push such efforts. The U.S. has a heavily privatized system, making health organizations highly competitive with one another. With no immediate way to change this, much of cyber-intelligence will be kept under wraps as a means of having the upper hand on adversaries. Proactive cybersecurity measures must overtake and outmatch the reactive measures that are commonly seen today. This requires improving a cohesive net of cybersecurity from top to bottom among all organizations participating in healthcare. Cybersecurity protocols that exist today have many goals and attempts at preventing cyber-attacks and keeping PHI secure[20]. Considering the growing number of EHR usage in the U.S., it is apparent that these protocols must be pushed to the next level in order to keep pace with potential threats.

VI. CONCLUSION

There is no universal EHR threat and no one approach to addressing the security concerns. As a relatively new field of study, there is very little research on the subject. It is important that security is designed into systems from the beginning, rather than being an afterthought. Utilizing the full advantages of new technologies, i.e. data mining and data warehousing, can help identify ongoing security violations and has potential for increasing the safety and security of EHRs. Encrypting all EHRs is not currently cost effective and is not necessary, as it is evident that certain types of information are at higher risk to specific threats. It is important for the healthcare industry to focus on security measures that are cost effective and resourceful, classifying and addressing the highest risk issues. The measures must also be flexible and scalable to adapt to changes in technology and healthcare practices. It is vital that the industry takes a methodical approach, testing and validating the effectiveness of security measures, in an attempt to avoid creating more problems in the long run. Cybersecurity for EHRs 33 While healthcare is clearly in an unenviable position today, with increasing pressure to implement EHRs and growing threats to the technology, it is not a losing battle. By taking a well informed and intelligent approach to security, the industry can learn quite a bit from the mistakes of other industries that have implemented technology without heeding security concerns. It is possible to proactively design and implement effective security measures for EHRs that will decrease and mitigate threats, ultimately decreasing the compromises and violations of patients' personal health information. With greater convenience and improved quality of documentation as a result of EHRs, it is sensible that these records are kept and maintained in a secure and private manner. One can argue that patients today have lost a bit of their privacy in the treatment of health care with the increasing facility of accessing and transferring information. However, it is still the right of every individual, whether they be patients, providers, or employees within healthcare organizations, to have control over who sees their personal health information and when and where it is seen. This right should not be lost in the age of government initiatives and widespread EHR implementation.

REFERENCES

[1] S. D. Hosek and S. G. Straus, *Patient privacy, consent, and identity management in health information exchange : issues for the military health system*. Santa Monica, Ca: Rand, 2013.

[2] T. U. Daim, Nima Behkami, Nuri Basoglu, O. M. Kök, and Liliya Hogaboam, *Healthcare Technology Innovation Adoption Electronic Health Records and Other Emerging Health Information Technology Innovations*. Cham Springer International Publishing, 2016.

[3] T. Qiu, L. Wang, and W. Zhao, *Quality, Reliability, Security and Robustness in Heterogeneous Systems : 13th International Conference, QShine 2017, Dalian, China, December 16 -17, 2017, Proceedings*. Cham: Springer International Publishing, 2018.

[4] L. Ayala, *Cybersecurity for hospitals and healthcare facilities : a guide to detection and prevention*. Berkeley, California: Apress, 2016.

[5] E. C. Ogu, *Cybersecurity for eHealth*. Routledge, 2022.

[6] A. H. Gantt and American Bar Association. Health Law Section, *Healthcare cybersecurity*. Chicago, Illinois: American Bar Association, Health Law Section, 2021.

[7] D. M. Tran, C. L. Thwaites, J. I. Van Nuil, J. McKnight, A. P. Luu, and C. Paton, "Digital Health Policy and Programs for Hospital Care in Vietnam: Scoping Review," *Journal of Medical Internet Research*, vol. 24, no. 2, p. e32392, Feb. 2022, doi: https://doi.org/10.2196/32392

[8] J. Scott, *Cybersecurity Hygiene for the Healthcare Industry*. CreateSpace, 2015.

[9] H.-C. Chang and Suliman Hawamdeh, *Cybersecurity for Information Professionals*. CRC Press, 2020.

[10] V. L. Patel, T. G. Kannampallil, D. R. Kaufman, and Springerlink (Online Service, *Cognitive Informatics for Biomedicine : Human Computer Interaction in Healthcare*. Cham: Springer International Publishing, 2015.

[11] S. P. Murphy, *Healthcare information security and privacy*. [New York]: McGraw-Hill Education, 2015.

[12] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, Lagkas, G. F. Fragulis, and A. Sarigiannidis, "A Self-Learning Approach for Detecting Intrusions in Healthcare Systems," *Zenodo (CERN European Organization for Nuclear Research)*, Jun. 2021, doi: https://doi.org/10.1109/icc42927.2021.9500354

[13] E J S Hovenga, H. Grain, and Ios Press, *Health information governance in a digital environment*. Amsterdam ; Washington, Dc: Ios Press, 2013.

[14] C. A. Shoniregun, K. Dube, and F. Mtenzi, *Electronic Healthcare Information Security*. Boston, Ma: Springer Us, 2010.

[15] B. P. Robichau, *Healthcare Information Privacy and Security Regulatory Compliance and Data Security in the Age of Electronic Health Records*. Berkeley, Ca Apress, 2014.

[16] T. W. Herzig, *Implementing Information Security in Healthcare*. HIMSS, 2013.

[17] J. J. Trinckes, *How healthcare data privacy is almost dead ... and what can be done to revive it!* Boca Raton, FL: CRC Press, Taylor & Francis Group, 2017.

[18] S. Tanwar, S. Tyagi, and N. Kumar, *Security and privacy of electronic healthcare records : concepts, paradigms and solutions*. London: Institution Of Engineering And Technology, 2019.

[19] F. D. Hudson, *Women securing the future with TIPPSS for connected healthcare : trust, identity, privacy, protection, safety, security*. Cham: Springer, 2022.

[20] Axel Wirth, (Security Strategist, C. Gates, and J. Smith, *Medical device cybersecurity for engineers and manufacturers*. Norwood, Ma: Artech House, 2020.

.