ISSN No:-2456-2165

Importance of Cybersecurity in Electronic Health Records

Rakesh Margam
Healthcare IT leader, Governors State University

Abstract:- The health of a nation's population is a leading indicator of that nation's level of economic output. When it comes to the provision of medical services, the effectiveness of various health care facilities is directly proportional to the state of patients' health. The medical records of patients require special attention because they are a vital part of the treatment audit trail prior to the implementation of the Electronic Health Record (EHR) system, patients' records were organized and archived through a record management system in a designated storage facility. The paper-based records were susceptible to inaccuracies resulting from illegible handwriting and occasionally proved inadequate in the context of prescriptions. In spite of its benefits, the EHR system introduced a new level of vulnerability by making it possible for dishonest individuals to gain access to the digital records including patients' personal information. This research paper's major goal is to conduct a study on the value of cybersecurity in EHRs, the difficulties associated with healthcare data vulnerability, and the significance of cybersecurity in those contexts. A survey method was used as the methodology for this research. The questionnaire was sent out to 196 respondents who are knowledgeable with EHR and work in the healthcare sector in a variety of places around the United States. According to the conclusions of this survey, all of the respondents (98%) were in agreement that significant components that need to be adopted to secure the EHR system include correct disposal of media, ownership of privileged accounts, periodic system audits, and identification and authentication mechanisms.

Keywords:- *Cybersecurity; Electronic Health Records (EHR); Health Care.*

I. INTRODUCTION

In recent years, there has been a rise in the number of individuals who exhibit concerns regarding the safeguarding of information. In recent times, the healthcare industry has been subjected to cyber-attacks, thereby eliciting concerns among stakeholders. In recent times, there has been a significant concern expressed about the prevalence of cyber-attacks targeting businesses operating in both the industry and consumer sectors. In recent times, the focus of discussion has been on the attacks targeted towards health systems and the potential vulnerabilities that have been exposed in certain critical medical devices, particularly those that are actively implantable and can be connected to a network [1,2]. When compared to other nations, such as the United States, many countries have been slower in effectively addressing cybersecurity issues. The healthcare industry in the United States is widely recognised as a sector, encompassing both its perception and operational aspects.

The approach adopted in the United States towards this issue is analogous to the approach taken towards the realms of industry and consumption. The matter, conversely, has only recently begun to garner the appropriate level of consideration [3]. The contemporary healthcare sector is characterized by a significant proliferation of cutting-edge technologies, such as artificial pancreas and pacemakers, which are integrated into the healthcare network. This integration involves over 300,000 categories of Medical Devices and is inextricably linked to the safety and effectiveness of the services provided, as well as the safeguarding of processed data. Consequently, this context necessitates a high level of vigilance [3].

➢ *Cybersecurity in Healthcare Sector:*

The cybersecurity in healthcare includes the following:

- DATA PRESERVATION: Data is accessible and functional for a long time. These methods must follow specifications and utilize appropriate informatics resources like robust filing systems.
- DATA ACCESS AND MODIFICATION: Typical functions like saving and retrieving database data. These acts are implemented through particular authentication and authorization procedures for regulated access.
- DATA EXCHANGE: The exchange of data can occur within the Hospital Local Area Network (LAN) or externally with citizens, healthcare practitioners, and other healthcare entities. Ensuring the safety, security, and compliance of security standards is imperative for data exchange.
- INTEROPERABILITY AND COMPLIANCE: Interoperability facilitates the exchange of data between various systems and devices, enabling healthcare professionals and individuals to share information seamlessly. Interoperability refers to the ability of different systems to exchange data and present it in a universally comprehensible manner. The concept of compliance pertains to adherence to established regulations. This pertains to the implementation of uniform standards (specifically, Dicom in radiology information systems) and adherence to both domestic and international regulations governing health information (such as GPRS in Europe) [4, 5].

ISSN No:-2456-2165

Hence, the issue of information security holds significant importance in the healthcare sector, with a majority of healthcare organizations prioritizing it. The acceptance of electronic health records further underscores the need for enhanced information security measures. The antecedent research relevant to this notion is expounded upon in greater detail in the subsequent section.

II. LITERATURE REVIEW

Table 1: Literature review

AUTHORS AND YEAR	METHODOLOGY	FINDINGS
(Mijwil et al., 2023) [6]	This study tried to incorporate ChatGPT in cybersecurity for the protection of medical information.	The primary objective of ChatGPT is to produce written content that simulates human-generated responses to a given inquiry or situation. The technology exhibits a diverse array of potential uses, encompassing chatbots, linguistic interpretation, automated text generation, and query resolution, among other examples.
(Wang & Alexander, 2021) [7]	The present study presents an overview of substantial technologies, including 5G, blockchain, telemedicine, and big data, that have been utilized to combat the COVID-19 pandemic, cyber-attacks, and cyber risks arising from both human actions and system and technology failures. The study also examines cybersecurity measures for telework, IoT, and telemedicine, as well as blockchain-based cybersecurity. The implementation of blockchain technology has been shown to provide protection to health systems against the COVID-19 pandemic while simultaneously enhancing privacy measures.	Telehealth compromises cybersecurity and privacy. Blockchain enhances digital health system privacy and pandemic management. The integration of blockchain and AI technologies has facilitated various applications in the healthcare industry such health data analytics, remote patient monitoring, electronic medical record (EMR) administration, and pharmaceutical supply chain management are some of the areas of focus in the healthcare industry.
(Kamerer & McDermott, 2020) [8]	This article addressed the primary cybersecurity challenges in healthcare, nurses' involvement in preventing and managing cybersecurity, and recommendations for nurses, educators, and regulators.	Patient PHI breaches have serious financial and personal consequences. Cybersecurity breaches affect healthcare organisations and staff. Healthcare technology is essential for nurses to preserve patient PHI.
(Argaw et al., 2020) [9]	This report provided examples of the attacks and how health organisations have responded.	Privacy-conscious data sharing and medical device security issues.
(Akarca et al., 2019) [10]	In health system reform methods, blockchain -based healthcare models strive to relate health care compensation to quality and patient-reported outcomes.	The utilization of digital technologies has been shown to enhance the accessibility, continuity, and calibre of healthcare and related services. The implementation of cybersecurity measures is imperative for the effective functioning of learning and value-based health systems.

According to the literature, information security is pervasive. Physical, administrative, and technical limitations are necessary for information security. The present study proposes a framework for bolstering electronic health record (EHR) security in financially constrained hospital settings. This framework encompasses administrative, physical, and technical measures to safeguard EHR information.

III. METHODOLOGY

The research was carried out using a methodology known as the questionnaire survey method. In this research, a cross-sectional exploratory research approach was used, which assisted in the collection of thoughts and replies from employees of health facilities who utilize EHR, which in turn assisted in the formulation of an information security model. The population of the study consisted of 196 individuals now employed in the health care industry in a variety of departments within the United States Department of Health and Human Services. The samples were chosen using a

method known as purposive sampling. The data was collected through the use of a standardised questionnaire based on the Likert scale. Two weeks before to the beginning of the actual data collection, the pilot questionnaires were given to a select group of 30 staff members. The team leaders were selected to assist in the distribution of the questionnaires to the members of their respective teams. The data that was collected was analysed with the help of basic SPSS.

IV. RESULTS AND DISCUSSIONS

The following headings might be used to provide further explanation of the findings of this study:

A. Importance & Advantages of Digitalisation:

To safeguard the availability, confidentiality, and integrity of a patient's medical and health information, reliable clinical applications and an IT infrastructure must be implemented. Due to the high number of healthcare professionals that require access, including nurses, doctors, and technicians, application-layer security must be monitored together with IT systems, employee communications, and policy violations. The IT security team is responsible for advancing information security information and event management (SIEM) by revealing any potential system or network vulnerabilities as a result of both internal and external attacks. Analysing threats in line with organisational mission and operating model is essential because of the impacts, which differ substantially across the government and industrial sectors.

The research of this study shows that security regulations set minimum security requirements for safeguarding EHRs. In order to secure patient information, the safety rule specifies administrative, technological, and physical security rules that must be implemented. If these are not followed, the system will face several security risks. Numerous vulnerabilities to the health facility's EHR systems have been identified through analysis. The EHR system is reported to be significantly threatened by unauthorised access, as indicated by a consensus of 93.5% of the respondents. An additional hazard that warrants consideration is social engineering, which accounts for 87.2% of the identified risks. file encryption (79.7%), record theft (80.8%), the use of counterfeit software (65.8%), input validation (61.5%), lack of backups (64.2%), blackouts (58.8%), access permissions not assigned (52.9%), lack of antivirus (54%), system failures (52.4%), errors brought on by a lack of technical support (49.2%), and lack of staff training (at 40%).

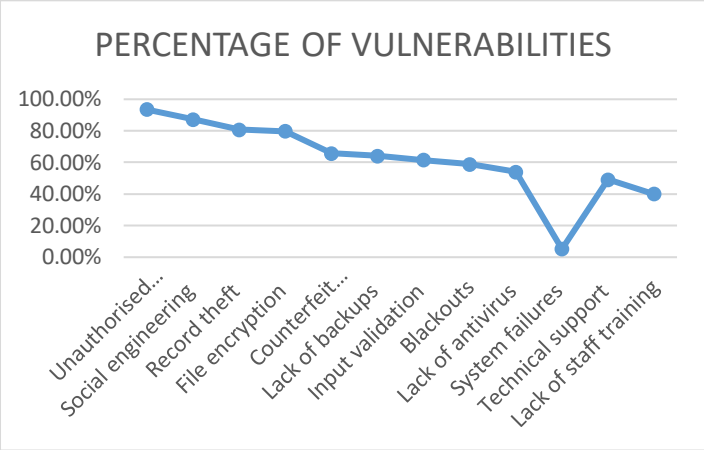

Fig 1: Percentage of Vulnerabilities

B. Cybersecurity In Us Healthcare System:

Three groups of individuals with a keen interest in medical and health information are jointly responsible for guaranteeing its protection.

- PRIVATE INDIVIDUALS: Security is mostly dependent on authentication. Patients may utilize biometrics to access their information since it is a method of measuring, evaluating, and exploiting physiological and behavioural features to identify an individual. It is more efficient than the use of passwords or PIN (personal identification number) codes in situations where the patient is too ill and unable to enter data or information because access is still possible. Even for young children and the elderly, this system would require proper training.

- GOVERNMENT: Certain concerns relating to the national security dangers in cyberspace are addressed by the National Strategy Forum and the American Bar Association Standing Committee on Law and National Security[1]. Not all dangers to national security originate in cyberspace, and not all of those threats spread to other countries. A number of computer crimes were made lawful in 1986 after the passage of the Computer Fraud and Abuse Act (CFAA)[2]. Government rules have been adopted in a number of nations in an effort to guarantee the sufficient protection of medical and health information worldwide. Several of these healthcare regulations are as follows:

  - According to the American Health Insurance Portability and Accountability Act (HIPPA)[3], healthcare providers are required to maintain and disclose PHI in accordance with proper systems and procedures.
  - The Health Information Technology for Economic and Clinical Health Act, a part of the American Recovery and Reinvestment Act (ARRA)[4] known as the Health Information Technology for Economic and Clinical

[1] https://www.americanbar.org/groups/law_national_security/
[2] https://www.nacdl.org/Landing/ComputerFraudandAbuseAct
[3] https://www.cdc.gov/phlp/publications/topic/hipaa.html
[4] https://www.fcc.gov/general/american-recovery-and-reinvestment-act-2009

Health Act (HITECH)[5]. By introducing additional rules regarding the confidentiality of EHRs, this act expands on HIPAA.

- The Federal Trade Commission (FTC)[6] has a rule known as the "Red Flags Rule" that requires healthcare providers to use procedures and security measures to prevent identity theft.

➢ HEALTHCARE ORGANISATIONS: The safeguarding of patient information is a component of risk management for medical, hospital, and health facilities. The first step in this process is the creation of a security committee to oversee the entire organisation. This committee should be made up of all medical staff, legal counsel, and the information technology team, though some healthcare facilities might contract with an outside company to secure their data. The following tasks must be completed by the security committee: risk analysis, management, application of policies and procedures, and risk monitoring.

C. Effectiveness of Security Measures Implemented And Proposed Additional Security Measures:

97% thought physical security worked. Automatic logoff had 46%, password implementation 36.9%, and multifactor authentication 29.4%. The consensus among all participants (98%) was that the incorporation of appropriate media disposal practises, privileged account ownership, regular system audits, and robust identification and authentication techniques would serve as the most effective security measures for enhancing the EHR system. The results indicate that a vast majority of participants, specifically 99%, expressed support for the implementation of system configuration and automated offsite backup. Additionally, a significant proportion of respondents, namely 95.2%, favoured the enhancement of physical security measures. Environmental security, including humidity, leakage, and temperature regulation, was approved by 94.7% of respondents, while 94.2% backed having enough generators and UPSs. 92.5% and 92% supported system maintenance and staff security. Aside from this, there are a variety of encryption methods accessible; the following four were the primary focus of central attention while they were performing their research, putting security in opposition to speed when it comes to application in a healthcare setting:

➢ DIGITAL SIGNATURES: Digital signatures verify document integrity. The digital signature serves as evidence that the entity responsible for its creation is the signatory and that the data has remained unaltered. The alteration of signed data results in the invalidation of the corresponding signature.

➢ HASHING TECHNIQUES: Hashing uses a cryptographic algorithm to mathematically turn one set of data into another of fixed length. A hash table maps data of any size to a specific length and stores it in the digest.

➢ SECOND LAYER AUTHENTICATION: The implementation of a security measure known as two-factor authentication (2FA) requires the presentation of two distinct forms of identification in order to obtain access to a specific resource. The initial authentication mechanism involves the use of a password, while the subsequent step typically entails the receipt of a code via SMS on the user's mobile device or the utilization of biometric identifiers such as fingerprints, facial recognition, or retinal scans to gain access to the Electronic Health Records platform, as mandated for each staff member.

➢ BLOCK CHAIN TECHNOLOGY: Blockchain has recently made a name for itself as a useful technology that has migrated to many different sectors. Figure 2 depicts the blockchain technology's system architecture.

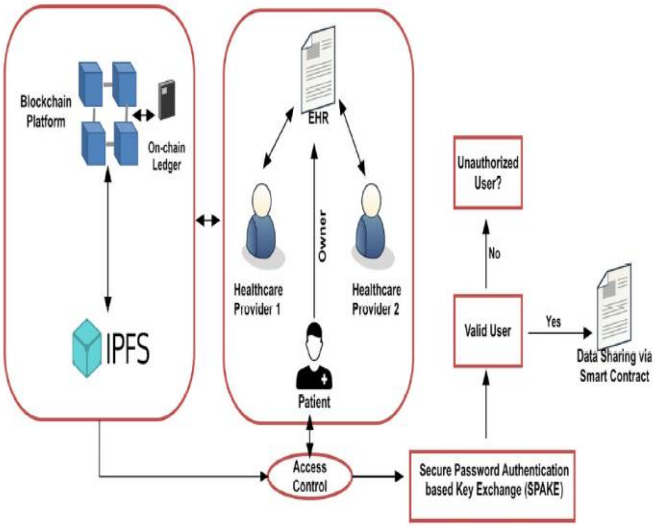

Fig 2: Block chain technology in Electronic Health Records protection [10]

V. CONCLUSION

The research investigated the influence of resource availability and organisational culture on the security of electronic health record (EHR) information. It is noteworthy that several characteristics or elements of the two moderating variables were already subsumed within the predictor variables and were not subjected to distinct analysis. The findings of this research indicate that the implementation of a singular control mechanism is inadequate in guaranteeing the security of the electronic health record (EHR) system. According to the model, the implementation of physical controls, administrative controls, and technical controls in isolation is insufficient to enhance the security of the electronic health record (EHR) system. However, the integration of these controls is deemed to be more effective in improving the overall security of the EHR system. According to research findings, the security of an information system is only minimally impacted by administrative controls and technological controls, respectively.

[5] https://www.hhs.gov/
[6] https://www.ftc.gov/

REFERENCES

[1]. Giansanti, D., & Monoscalco, L. (2021). The cyber-risk in cardiology: Towards an investigation on the self-perception among the cardiologists. *Mhealth*, *7*.
[2]. Giansanti, D., Grigioni, M., Monoscalco, L., & Gulino, R. A. (2020). A smartphone based survey to investigate the cyber-risk perception on the health-care professionals. In *XV Mediterranean Conference on Medical and Biological Engineering and Computing–MEDICON 2019: Proceedings of MEDICON 2019, September 26-28, 2019, Coimbra, Portugal* (pp. 914-923). Springer International Publishing.
[3]. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cybersecurity and digital transformation. *Technovation*, *121*, 102583.
[4]. Zhu, S., Saravanan, V., & Muthu, B. (2020). Achieving data security and privacy across healthcare applications using cybersecurity mechanisms. *The Electronic Library*, *38*(5/6), 979-995.
[5]. Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: an analysis of FDA product summaries. *BMJ open*, *9*(6), e025374.
[6] Mijwil, M., Aljanabi, M., & Ali, A. H. (2023). ChatGPT: exploring the role of cybersecurity in the protection of medical information. *Mesopotamian journal of cybersecurity*, *2023*, 18-21.
[7]. Wang, L., & Alexander, C. A. (2021). Cybersecurity during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, *5*(2), 146-157.
[8] Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, *10*(4), 48-53.
[9]. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, 1-10.
[10] Akarca, D., Xiu, P. Y., Ebbitt, D., Mustafa, B., Al-Ramadhani, H., & Albeyatti, A. (2019, June). Blockchain secured electronic health records: patient rights, privacy and cybersecurity. In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 108-111). IEEE.