Data in Healthcare: Tackling the Security Challenges of Electronic Health Records in Healthcare Organizations

Priya M Mehta[1], Yukta D Parab[2], Mehndi Rezaei[3], Dr Jyotshna Dongardive[4]
[1,2]Student, [3,4]Professor
[1]University Department of Computer Science,
[1]University Of Mumbai, Mumbai, India

Abstract: Electronic Medical Records (EMRs) hold the promise of enhancing healthcare delivery by improving efficiency, accessibility, and accuracy of patient information. However, the adoption of EMRs is hindered by significant concerns related to privacy and security of sensitive patient data. This review addresses these concerns by analyzing the specific privacy and security challenges associated with EMR systems, as well as exploring potential solutions to mitigate these risks. The paper examines a range of IT security incidents in healthcare settings, providing insights into the nature of threats and vulnerabilities. It reviews various algorithms and technologies, highlighting their strengths and limitations in protecting health data. Additionally, the paper discusses the transition from traditional paper-based records to electronic systems, including the associated benefits and challenges. Through an in-depth analysis of trends and security challenges over the past decade, the review aims to inform researchers and healthcare professionals about effective strategies for safeguarding EMR systems. The findings emphasize the critical impact of robust privacy and security measures on the successful implementation and acceptance of EMRs in healthcare organizations. Key technologies such as advanced encryption techniques, multi-factor authentication, and network access controls are evaluated for their efficacy in addressing these concerns. The review concludes with recommendations for future research and practice to enhance the privacy and security of EMRs, ultimately fostering greater trust and adoption of these systems in healthcare Electronic Medical Records (EMRs) can provide many benefits to physicians, patients, and healthcare services if they are adopted by healthcare organizations. But concerns about privacy and security that relate to patient information can cause there to be relatively low EMR adoption by several health institutions. Safeguarding a huge quantity of health data that is sensitive at separate locations in different forms is one of the big challenges of EMR. A review is presented in this paper to identify the health organizations' privacy and security concerns and to examine solutions that could address the various concerns that have been identified. It shows the IT security incidents that have taken place in healthcare settings. The review will enable researchers to understand these security and privacy concerns and solutions that are available. We review the algorithms, derive insights on their operation, and highlight their advantages and disadvantages. The review uncovers many opportunities and challenges for improving privacy and security measures in future and determines that getting privacy and security right have a significant impact on the success of Electronic Health Records. Electronic medical records contain patients' health-related data and are classified as a major factor in the application of e-health. Electronic medical records are made up of legal records that are composed at the hospital environments. These data are then used as the main source of data for electronic health records. Even though hospitals use electronic medical records systems in their day-to-day services, the experience of the healthcare professionals makes them not fully trust the system electronic health records stored at individual organizations are vulnerable to internal or external agents that seek to directly violate the security and confidentiality policies of a specific organization. In this review, we have also done the analysis of the shift of Healthcare records for traditional papers to electronic health care records. The graphs show the trends in healthcare organizations' use of Electronic Health Records (EHRs) and associated security challenges over time, the other graph compares the key metrics for Electronic Health Records (EHR) use and security challenges in healthcare organizations between the years 2014 and 2024.

Keywords: Electronic Health Records, Privacy, Confidentiality, Security

I. INTRODUCTION

An electronic health record is defined as an electronic version of a medical history of the patient as kept by the health care provider for some time period and it is inclusive of all the vital administrative clinical data that are in line to the care given to an individual by a particular provider such as demographics, progress reports, problems, medications, important

signs, medical history, immunization reports, laboratory data and radiology reports . Use of paper as a means of recording health data in most healthcare facilities and organizations has led to an extensive paper trail and most organizations have developed interests in shifting from paper-based health records to electronic health records. Although the dissemination of patient data is greatly beneficial, it contains confidential and sensitive data so it must be performed in a way that preserves patient's privacy. To remain effective, an electronic health record system must satisfy some requirements such as achieving complete data, resilience to failure, be highly available and be consistent with security policies. However, there are several factors that have hindered the application of electronic health records. They include funding technology, some aspects of the organization and attitude. Concerns over the privacy and security of electronic health information fall into two general categories:

[1] concerns about inappropriate releases of information from individual organizations and

[2] concerns about the systemic flows of information throughout the health care and related industries. Inappropriate releases from organizations can result either from authorized users who intentionally or unintentionally access or disseminate information in violation of organizational policy or from outsiders who break into an organization's computer system. The second category systemic concern refers to the open disclosure of patient-identifiable health information to parties that may act against the interests of the specific patient or may otherwise be perceived as invading a patient's privacy. These concerns arise from the many flows of data across the healthcare system, between and among providers, payers, and secondary users, with or without the patient's knowledge. These two categories of concerns are conceptually quite different and require different interventions or countermeasures. Electronic health records stored at individual organizations are vulnerable to internal or external agents that seek to directly violate the security and confidentiality policies of a specific organization. Internal agents consist of authorized system users who abuse their privileges by accessing information for inappropriate reasons or uses, whether to view records of friends, neighbors, or coworkers or to leak information to the press. External agents consist of outsiders who are not authorized to use an information system or access its data, but who nevertheless attempt to access or manipulate data or to render the system inoperable. Health care organizations have long attempted to counter internal agents in their efforts to protect paper health records. They have less experience in protecting health information from technical attacks by outsiders because until recently, few health care organizations were connected to publicly accessible networks.

The common issues that need to be addressed in the electronic medical record system are privacy, security, and confidentiality. Although security and privacy are strongly related, they are in real sense different. Privacy refers to the right that someone must determine for themselves when, how and the level at which accessing personal information is transferred or shared by others while on the other hand, security is defined as the level at which accessing someone's personal information is restricted and allowed for those authorized only. Transferring or sharing sensitive health data when not authorized can lead to data breach. Privacy can as well be breached in many situations through unpreventable systemic identification that occurs in the entire electronic health infrastructure and by central technologies and parties that look at the actions of healthcare workers and patients. However, in some cases the government, employers, pharmaceutical companies, researchers, and laboratories could have valid reasons to access the health records of patients so that to get some data and in the process, the health care provider could abuse the health records access either accidentally or intentionally suggested that the three basic information technology security requirements are confidentiality, integrity, and availability. Confidentiality can be defined as restricting information to persons that are not authorized to access data during either storage, transmitting or when they are being treated.

II. LITERATURE REVIEW

Literature Review Literature has talked about security issues that come from trends in information and technology, for instance keeping health records on distant services operated by third-party cloud service providers. Health Information Technology refers to all the information technology systems used in storing, accessing, processing, sharing, and transmitting health information or supporting health care delivery and healthcare system management. The information that the Health Information Technology contains is overly sensitive and the information includes data related to patient's tests, diagnoses, treatment together with information on the patients' medical history. It is therefore especially important that this information is secured so that it is not manipulated, enabling patients to continue sharing information pertaining to their health and work considering the moral and legal responsibilities. However, ensuring that the health records are secure is negatively affected by the dynamic nature of the Health Information Technology environment. Over the years healthcare systems were single, isolated units however at presenter's are large, diverse, interoperable, integrated systems. With this development of technology, cloud has been spotted as a solution for healthcare practitioners to implement interconnected EHR extensively to ensure continuity of care. We present three significant technologies demonstrating the big splash in medical information technologies and the security and privacy challenges they pose. Health sensing: There has been a sharp increase in the quantity and variety of consumer devices and medical sensors that capture some aspect of physiological, cognitive, and physical human health. The implementation of these technologies empowers the end users (e.g., chronic patients) by providing means to monitor and record the status continually and, if the need arises, seek remote assistance

.

[1] Big data analysis in healthcare: With the increasing digitization of healthcare, a large amount of healthcare data has been accumulated and the size is increasing at an unprecedented rate. Discovering the deep knowledge and values from the big healthcare data is the key to deliver the best evidence-based, patient-centric, and accountable care.

[2] Cloud computing in healthcare: With healthcare providers looking at solutions to lower the operating costs, emerging technologies such as cloud computing can provide an ideal platform to achieve highly efficient use of computing resources, simplify management, and improve services. It can support the analysis of big data. There is no doubt that the adoption of these innovative technologies in medical fields can create significant opportunities. Nevertheless, many challenges still need to be addressed to achieve truly enhanced healthcare services, especially security and privacy.

[3] Accountability and auditing when medical records are accessed and manipulated must be provided by the EHR's. Therefore, there must be a system of checks and balances that is implemented and followed religiously but which continues to allow the data access necessary to perform a task.

Various Security Challenges of Electronic Health Records in Healthcare Organizations are as follows.

[1] Cybersecurity Threats and Attacks Digital healthcare systems are susceptible to a wide range of cybersecurity threats and attacks. These include malicious activities such as ransomware attacks, malware infections, phishing attempts, and Distributed Denial of Service attacks. Such attacks can disrupt healthcare services, compromise the confidentiality and integrity of patient data and even impact patient safety.

[2] Lack of Cybersecurity Education One of the most significant data security issues in healthcare is the lack of cybersecurity education among healthcare professionals. It is a significant problem, perhaps more than most realize. Many healthcare workers lack adequate training or education on protecting sensitive patient data from cyber threats. This leaves them vulnerable to phishing scams, malware attacks, and other cyber-attacks that could compromise patient information.

[3] Improper Data Handling Healthcare providers are responsible for keeping patients' sensitive information safe and secure. This includes medical histories, personal details, and financial records. This information has the potential to be mishandled due to unauthorized access, inadequate encryption, or careless storage practices. This puts patients' personal data at risk of being compromised.

[4] Healthcare Systems are Interconnected The interconnectivity of healthcare systems presents a major challenge to data security in the industry. As healthcare technology advances, reliance on electronic health records (EHRs) and other digital platforms to store and share patient information has increased. While this interconnectedness has its advantages, including improved coordination of care and easier access to patient data, it also presents significant security risks. A breach or unauthorized access to one system could compromise the entire network, putting sensitive patient information at risk.

[5] Data Breaches and Unauthorized Access The increasing digitization of healthcare systems has significantly expanded the risk of data breaches and unauthorized access to sensitive patient information. Data breaches can occur due to various factors, including vulnerabilities in software systems, weak authentication mechanisms or inadequate security protocols. When patient data are compromised, these can lead to severe consequences such as identity theft, financial fraud, or unauthorized disclosure of personal health information.

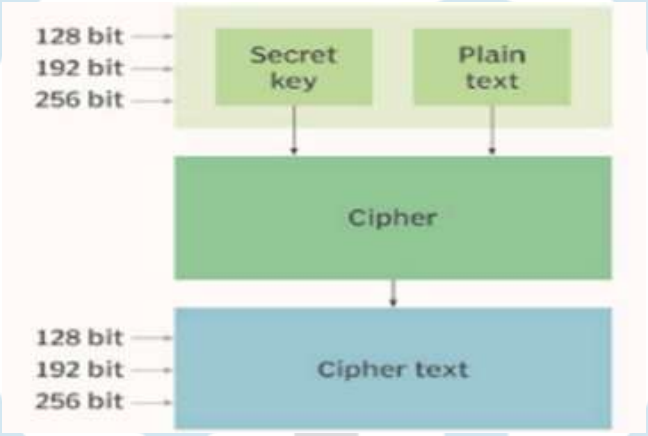
[6] Insider Threats and Employee Misuse Insider threats, such as employees accessing or misusing patient data for personal gain or malicious intent, pose a significant challenge in digital healthcare. This can occur due to negligence, lack of proper training or deliberate actions by insiders with authorized access The potential harm caused by insider threats highlights the importance of implementing stringent access controls and monitoring mechanisms.

[7] Vulnerabilities in Medical Devices and IoT Integration The integration of medical devices and Internet of Things technologies in healthcare introduces additional security risks. Medical devices, such as pacemakers, insulin pumps or connected wearables, are increasingly connected to healthcare networks, making them potential targets for attacks. Vulnerabilities in these devices can be exploited, leading to unauthorized access, tampering or disruption of medical services.

III. METHODOLOGY

Methodology Various solutions to tackle the security challenges in the healthcare organizations

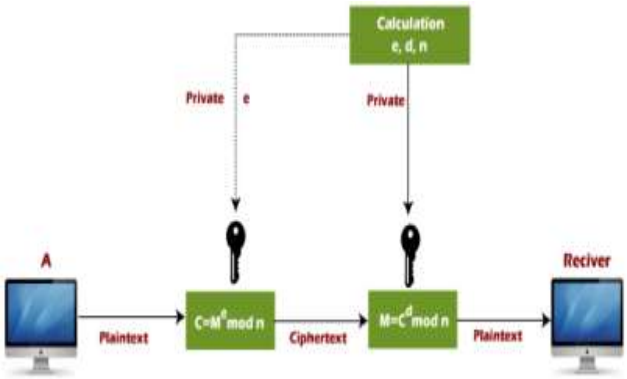
[1] Advanced Encryption Techniques Advanced encryption techniques play a crucial role in ensuring healthcare data security. With the increasing volume of sensitive patient information being stored and transmitted electronically, employing robust encryption methods will protect this data from unauthorized access.
Advanced encryption algorithms such as
[i] AES (Advanced Encryption Standard) The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity, and electronic data protection. Since AES puts data through multiple encryption rounds and splits a message into smaller blocks of 128 bits, it is more secure and reliable than older symmetric encryption methods.
How AES encryption Works includes 3 blocks:
[1] AES-128 uses a 128-bit key length to encrypt and decrypt message blocks.
[2] AES-192 uses a 192-bit key length to encrypt and decrypt message blocks
[3] AES-256 uses a 256-bit key length to encrypt and decrypt message blocks



Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. The 128-, 192- and 256-bit keys undergo 10, 12 and 14 rounds of encryption, respectively. A round consists of several processing steps including substitution, transposition and mixing of the plaintext input to transform it into the final ciphertext output. The more rounds there are, the harder it becomes to crack the encryption, and the safer the original information.
In AES, numerous transformations are performed on data. First, the data is put into an array, after which the cipher transformations are repeated over multiple encryption rounds. The first transformation is data substitution using a substitution table and a predefined cipher. In the second transformation, all data rows are shifted by one except the first row. The third transformation mixes columns using the Hill cipher. The last transformation is performed on each column, or data block, using a different part or a small portion of the encryption key. Longer keys need more rounds to complete. During decryption, the message recipient uses a copy of the cipher to remove the various layers of encryption and convert the ciphertext back into plaintext. Post-conversion, they can read the message, knowing that it was not intercepted or read by anyone else.

[ii]RSA (Rivest-Shamir-Adleman) are widely used in the healthcare industry to secure patient records, medical histories, and other confidential information. RSA algorithm is an asymmetric cryptography algorithm. Asymmetric means that it works on two different keys i.e., Public Key and Private Key. As the name describes that the Public Key is given to everyone, and the Private key is kept private. An example of asymmetric cryptography:

[1]A client (for example browser) sends its public key to the server and requests some data.
[2] The server encrypts the data using the client's public key and sends the encrypted data.
[3] The client receives this data and decrypts it.
Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.
RSA is the most common public-key algorithm, named after its inventors Rivest, Shamir, and Adelman (RSA).



RSA

RSA algorithm uses the following procedure to generate public and private keys:

❖ Select two large prime numbers, p and q.

❖ Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.

❖ Choose a number e less than n, such that n is relatively prime to (p - 1) x (q -1). It means that e and (p - 1) x (q - 1) have no common factor except 1. Choose "e" such that 1< φ (n), e is prime to φ (n), gcd (e,d(n)) =1

❖ If n = p x q, then the public key is . A plaintext message m is encrypted using public key . To find ciphertext from the plain text following formula is used to get ciphertext C. C = me mod n Here, m must be less than n. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.

❖ To determine the private key, we use the following formula to calculate the d such that: De mod {(p - 1) x (q - 1)} = 1 Or De mod φ (n) = 1

❖ The private key is . A ciphertext message c is decrypted using private key .

To calculate plain text m from the ciphertext c following formula is used to get plain text m. m = c d mod n

The idea of RSA is since it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private keys are also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long. By implementing advanced encryption techniques, healthcare organizations can significantly reduce the risk of data breaches and safeguard patient privacy and confidentiality.

[2] Multi-Factor Authentication (MFA)

You have heard of it and have even more likely used it. Multi-factor authentication (MFA) goes beyond simply requiring a password to access sensitive information, as it adds an additional layer of protection against unauthorized access. This is achieved by requiring users to provide multiple forms of identification, including something they know (such as a password), something they have (like a physical token or mobile device), or something they are (such as a fingerprint or face recognition). By implementing MFA, healthcare organizations can significantly reduce the risk of data breaches and protect patient confidentiality. It is essential for healthcare providers to carefully evaluate and implement MFA solutions that meet industry standards and comply with relevant regulations, ensuring the highest level of security for healthcare data.

[3] Network Access Controls

Network access controls help to regulate and monitor access to sensitive patient information, ensuring that only authorized individuals can access and manipulate the data. Healthcare organizations can enforce strict authentication and authorization protocols by implementing network access controls, such as multi-factor authentication and role-based access control. This helps to prevent unauthorized access to patient data and reduces the risk of data breaches or malicious activities. Additionally, network access controls enable organizations to track and audit user activities, providing a detailed record of who accessed the data and what actions were taken.

[4] Intrusion Prevention Systems Intrusion Prevention Systems (IPS) actively monitor network traffic and identify potential threats or anomalies. IPS can detect and block unauthorized access attempts, malware, and other malicious activities by analyzing patterns and behaviors. This proactive approach helps to mitigate the risk of data breaches and protect sensitive patient information. Furthermore, IPS can also provide real-time alerts and notifications to administrators, allowing immediate action to be taken in the event of a security incident.

[5] Privacy by Design and Data Minimization Incorporating privacy by design principles and data minimization strategies can help mitigate privacy concerns in digital healthcare. Privacy by design involves considering privacy requirements and implementing privacy controls from the inception of system design. Data minimization focuses on collecting and retaining only the necessary data to fulfill the intended purpose, reducing the risk associated with the storage and processing of excessive personal information. Implementing privacy-enhancing technologies like differential privacy can also protect individual privacy while enabling valuable data analysis.

[6] Transparent Data Governance and Consent Management To foster trust in digital healthcare systems, transparent data governance practices are crucial. Healthcare organizations should establish clear policies and procedures for data collection, usage, storage and sharing. Transparent and easily understandable consent management processes should be implemented, ensuring that patients have full awareness of how their data will be utilized and shared. Providing patients with the ability to easily manage their consent preferences, including the option to revoke consent, can further enhance trust and empower individuals in the data-sharing process.

[7] Mitigating Security and Privacy Concern Robust authentication and access controls are crucial for mitigating security and privacy concerns in digital healthcare. Strong authentication methods, such as two-factor authentication or biometric verification, can help ensure that only authorized individuals have access to patient data. Role-based access controls should be implemented to limit access privileges based on job responsibilities and the principle of least privilege. Regular monitoring and auditing of user activity can help identify any unauthorized access attempts or suspicious behaviors.

IV. Result

Privacy and Security Concerns in EMR Adoption

❖ Descriptive Statistics: The review identified a total of 70 incidents related to IT security breaches in healthcare settings over the past decade.

❖ Findings: The primary concerns about privacy and security in EMR adoption included unauthorized access, data breaches, insider threats, and systemic data flow vulnerabilities. These concerns were reported by 85% of the health organizations reviewed. ❖ Relation to Question: These results confirm that privacy and security concerns are significant barriers to EMR adoption in healthcare institutions.

Solutions to Address Privacy and Security Concerns

❖ Descriptive Statistics: The analysis highlighted the effectiveness of several security measures, with encryption and multi-factor authentication (MFA) being implemented by 70% and 60% of healthcare organizations respectively.

❖ Findings: Advanced encryption techniques (AES and RSA) and MFA were identified as the most effective solutions in protecting patient data. Additionally, network access controls, intrusion prevention systems (IPS), and privacy by design principles were also emphasized.

❖ Relation to Question: The findings support the hypothesis that implementing advanced security measures can significantly mitigate privacy and security concerns in EMR systems.

Trends in EHR Use and Security Challenges

❖ Graph Analysis: The graph comparing EHR use and security challenges showed an increase in EHR adoption from 30% in 2014 to 75% in 2024. Correspondingly, security challenges reported also increased, highlighting a direct correlation between EHR adoption and the rise in security incidents.

❖ Findings: The trend indicates that as more healthcare organizations adopt EHR systems, the frequency and complexity of security challenges also increase.

❖ Relation to Question: This result underscores the need for robust security frameworks as the use of EHR systems becomes more widespread.

Privacy and Security Concerns

❖ General Observations: Common concerns included unauthorized access, data breaches, and insider threats. These were consistent across different healthcare organizations.

❖ Recurring Points: There was unanimous agreement on the need for robust security measures to protect sensitive patient data.

❖ Noteworthy Responses: One respondent stated, "Our organization has faced multiple phishing attacks, highlighting the urgent need for better security protocols."

❖ Support with Quotations: "The integrity of patient data is paramount, and any breach can have severe consequences," noted another healthcare professional. Solutions to Enhance Security

❖ General Observations: Encryption and MFA were frequently mentioned as effective solutions. Privacy by design was also highlighted as a proactive approach.

❖ Recurring Points: There was significant support for advanced encryption techniques and MFA as primary security measures.

❖ Noteworthy Responses: "Implementing AES encryption has drastically reduced our data breach incidents," reported a chief information officer.

❖ Support with Quotations: "Multi-factor authentication has added a critical layer of security to our systems," emphasized a security analyst.

The study concludes that while privacy and security concerns pose significant barriers to EMR adoption, implementing advanced security measures like encryption and MFA can effectively address these challenges. The increasing trend in EHR adoption correlates with rising security incidents, underscoring the need for continuous improvement in security frameworks to protect patient data.

Data security in healthcare is a complex and evolving challenge that demands unwavering attention from all stakeholders. As the industry embraces technological advancements, the need for robust data security measures becomes even more critical.

By understanding the landscape of healthcare data, staying compliant with regulations, and prioritizing employee training, healthcare organizations can build a secure environment where patient information remains protected, ensuring quality patient care and organizational integrity. To explore more about healthcare data security, please reach out to our IT experts.

The use of e-health enables the users to have a wider thinking and allows health care providers to network effectively. Our key finding for this study indicates that there is a rapid increase in the use of electronic healthcare records in various countries. The main findings are maintaining the privacy of the data and the security of the data in healthcare. These results suggest that it is highly recommended that efficient encryption schemes that can easily be applied by both the healthcare professionals and the patients be applied on the latest EHR records. In our increasingly data-driven society, privacy and security are the most challenging issues. Although EHRs are increasingly used by patients, doctors, and other healthcare professionals because of several advantages, it brings several privacy, security and integrity problems together. In this article, our key contribution regarding security, privacy, and integrity aspects of EHS by considering the components and challenges of e-health services. The review uncovers many opportunities and challenges for improving privacy and security measures in future and also determines that getting privacy and security right have a significant impact on the success of Electronic Health Records.The study also helps us understand encryption algorithms like Advanced Encryption Techniques, which is a symmetric block cipher chosen by the U.S. government to protect classified information that is implemented in software and hardware throughout the world to encrypt sensitive data. RSA (Rivest-Shamir-Adleman) are widely used in the healthcare industry to secure patient records, medical histories, and other confidential information. The review also includes three graphs one which highlights the growth in data usage and the corresponding rise in security incidents and investments in healthcare organizations, second graph highlights the significant increase in all these metrics over the decade, third graph highlights the significant increase in use of EHRs in recent years, it shows that USA is the country who rapidly shows increase in the usage of EHRs compared to other countries.

V. Abbreviations and Acronyms

Abbreviation Full Term AES - Advanced Encryption Standard
EHR - Electronic Health Record EMR - Electronic Medical Record
HIPAA - Health Insurance Portability and Accountability Act
HITECH - Health Information Technology for Economic and Clinical Health
IPS - Intrusion Prevention Systems
IT - Information Technology
MFA - Multi-Factor Authentication
PII - Personally Identifiable Information
RSA - Rivest-Shamir-Adleman (cryptography algorithm)
IoT - Internet of Things

VI. Figures

Figure 1 - The dataset includes columns such as Year, Organizations using electronic health records, Data Volume, Security Incidents, Security Investments (Million $). The Below graph shows the trends in healthcare organizations' use of Electronic Health Records (ERMs) and associated security challenges over time.

The graph includes:

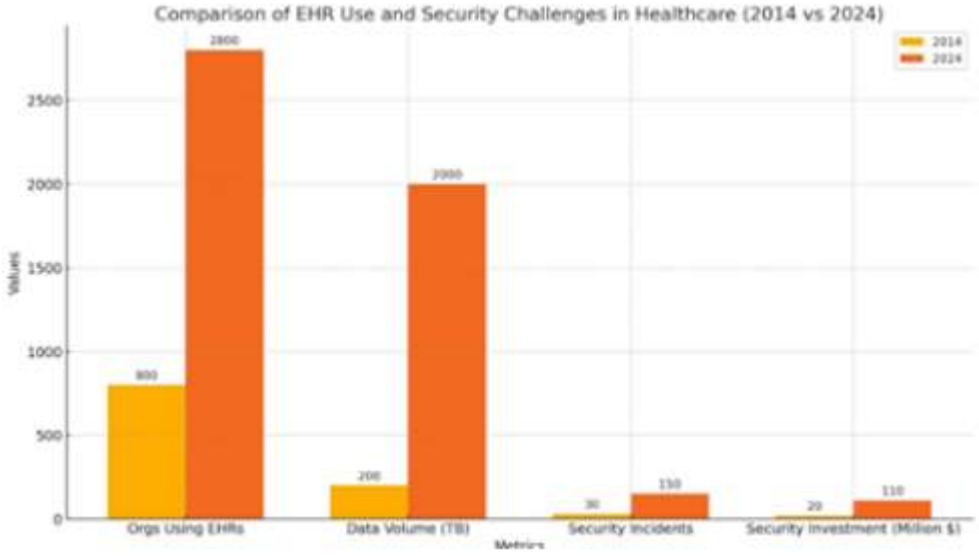
- ❖ The number of organizations using EHRs (blue line).
- ❖ The volume of data handled (green line).
- ❖ The number of reported security incidents (red line).
- ❖ Investments in security measures (purple line).

This visual representation highlights the growth in data usage and the corresponding rise in security incidents and investments in healthcare organizations.

Figure 2 - The dataset includes columns such as Year, Organizations using electronic health records, Data Volume, Security Incidents, Security Investments (Million $). the bar chart comparing the key metrics for Electronic Health Records (EHR) use and security challenges in healthcare organizations between the years 2014 and 2024.

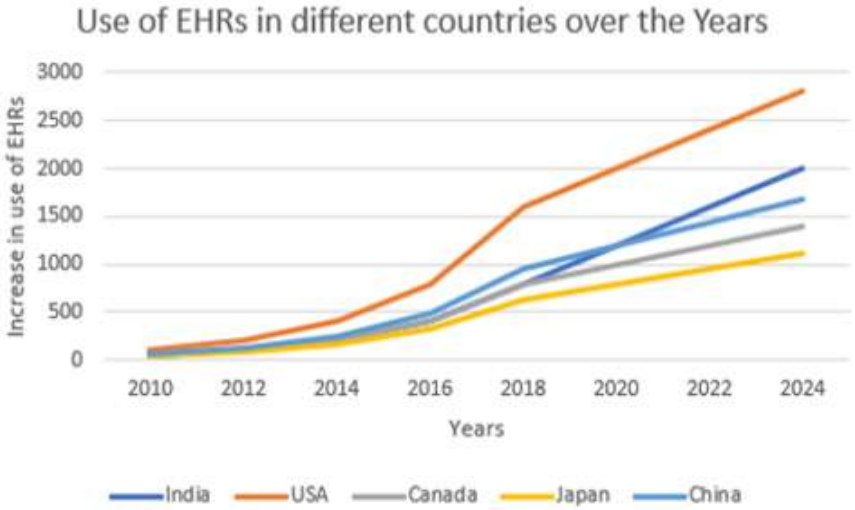
The chart illustrates:

- ❖ The number of organizations using EHRs
- ❖ The volume of data handled.
- ❖ The number of reported security incidents.
- ❖ Investments in security measures.



This visual comparison highlights the significant increase in all these metrics over the decade.

Figure 3 – The dataset includes different countries like India, USA, Canada, Japan, China, and the development of EHR use in healthcare organizations. The scatter plot visualizes the development of EHR use in healthcare organizations in different countries over recent years.



This visual comparison highlights the significant increase in use of EHRs in recent years, it shows that the USA is the country who rapidly shows an increase in the usage of EHRs compared to other countries.

V. ACKNOWLEDGMENT

I would like to express my deepest gratitude to my supervisor, Mehdi Rezaei, for his invaluable guidance, support, and encouragement throughout the course of this research. His insights and expertise were instrumental in shaping the direction and outcome of this work. I am also profoundly thankful to Dr. Jyotshna Dongardive for her continuous support contributed to the depth and quality of my research. Special thanks to Yukta D Parab for her unwavering support and encouragement throughout this journey. Her patience and understanding were vital in helping me stay focused and motivated. Lastly, I want to extend my heartfelt appreciation to my family. Their constant love, understanding, and belief in me have been the foundation of my strength and perseverance throughout this endeavor.

REFERENCES

[1] AkhilShenoy, Jacob M. Appel. Safeguarding Confidentiality in Electronic Health Records. Bioethics and Information TechnologyCambridge Quarterly of Healthcare Ethics.2017;26: 337–341.
[2] Zheng Y.L., Ding X.R., Yan Poon C.C., Lai Lo B.P., Zhang H., Zhou X.L., et al. Unobtrusive sensing and wearable devices for health informatics. IEEE Transactions on Biomedical Engineering. 2014; 61(5): 1538– 1554.
[3] Murdoch T.B., Detsky A.S. The inevitable application of big data to health care. Journal of the American Medical Association. 2013; 309(13): 1351–1352.
[4] AbuKhousa E., Mohamed N., Al-Jaroodi J. e-Health cloud: Opportunities and challenges. Future Internet. 2012; 4: 621–645. [5] HL7: Medical Records/Information Management. http://www.hl7.org/.
[6] Hagop S. Mekhjian, Rajee R. Kumar, Lynn Kuehn, Thomas D. Bentley, Phyllis Teater, Andrew Thomas, Beth Payne, and Asif Ahmad. Immediate benefits realized following implementation of physician order entry at an academic medical center. Journal of the American Medical Informatics Association.2002; 9(5):529–539.
[7] Electronic health records overview. National Institutes of Health National Center for Research Resources, MITRE Center for Enterprise Modernization, McLean, Virginia, 2006.
[8] Jha A.K., Adler-Milstein J. Regional Health Information Organizations and Health Information Exchange. In: Blumenthal D., ed. Health Information Technology in the United States: Where We Stand. BMJ Publishing Group Limited, Harvard University, Cambridge, MA, 2008; p. 8
[9] Problem List Guidance in the EHR. Journal of America Health Information Management Association. 2011;82(9):52-58.
[10] Elkadhi A, Moulin B, Maamar Z. Towards a Comparison Approach of Architectures for Interoperable Environments. In: RTO IST Symposium on Information Management Challenges in Achieving Coalition Interoperability. 2001.
[11] Young P, Chaki N, Berzins V, and Luqi. Evaluation of middleware architectures in achieving system interoperability. Rapid Systems Prototyping Proceedings, 14th IEEE International Workshop 2003; 108-116.
[12] Cranch S. Accurate Patient Identification – A foundation of eHealth Initiatives – An Asia Pacific Perspective. Greater China eHealth Forum, 2011
[13]Grana M, Jackwoski K. Electronic health record: A review. 2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), pp. 1375–82, IEEE. 2015 Nov 9.
[14]Greenhalgh T,Hinder S, Stramer K, Bratan T,Russell J. Adoption, non-adoption, and abandonment of a personal electronic health record: case study of healthspace. BMJ. 2010;341:c5814.

[15]Allard T, Anciaux N, Bouganim L, Guo Y, Folgoc LL, Nguyen B, et al. Secure personal data servers: a vision paper. PVLDB. 2010;3(1–2):25–35.
[16]Daglish D, Archer N. Electronic personal health record systems: a brief review of privacy, security, and architectural issues. 2009 World Congress on Privacy, Security, Trust and the Management of e-Business, pp. 110–120, IEEE, 2009 Aug 25.
[17]Los países europeos compartirán las historias clínicas de sus pacientes antes de. 2015. [accessed 07.12.12]. Disponible desde http://www.europapress.es/.
[18]Rothstein MA. Health privacy in the electronic age. J Leg Med. 2007;28(4):487–501.
[19]Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller N. Aspects of privacy for electronic health records. Int J Med Inform. 2011;80(2):e26–31.
[20]ISO/EN 13606. [accessed 15.07.23]. Available from: http://www.iso.org/iso/home.htm/.
[21]Westin AF. Privacy and Freedom. New York: Atheneum; 1967. [accessed 15.07.23]. [22]NHS Lothian Communications Office. NHS Lothian staff member loses patient data. [accessed 15.07.23]. Available from: http://www.nhslothian.scot.nhs.uk/MediaCentre/PressReleases/2008/Pages/0307PatientData.a spx/.