Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2023, 10(1):61-66**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Healthcare Information Security Combat, Wrestling with Challenges

Santosh S Deshmukh

PMP, SCM, MSBA, Senior Member, IEEE

Abstract Securing data is crucial in healthcare because of the confidentiality, sensitivity, and personal characteristics of the information (PHI) being handled. This paper will give a wide overview of the continuing combat between healthcare information and security breaches. The degree of security challenges is in proportion to the availability of the production of healthcare information. The gradual increase in data in the last few decades boosted security challenges enormously. This paper explains the background of these challenges, the way out, and possible future options to wrestle with these challenges. Finally, a few suggestions that might work and improve the overall security of healthcare information. This paper will also discuss emerging Blockchain technology and its stake in enhancing the security of information. The research explores security challenges in deploying e-healthcare systems with existing medical standards and offers strategies and advice to ensure the protection and advancement of e-healthcare or intelligent healthcare services. Healthcare information security is the comprehensive protection of patient data within the healthcare sector. It encompasses measures to safeguard electronic health records (EHRs), prevent unauthorized access, and ensure compliance with rigorous privacy regulations like HIPAA. The goal is to maintain the confidentiality, integrity, and availability of sensitive medical information, protecting patient privacy and trust. Robust security protocols, incident response plans, and ongoing staff training are vital components. With the increasing digitization of healthcare records, information security plays a critical role in mitigating evolving cyber threats, fostering interoperability, and upholding the ethical responsibility to safeguard patient well-being and confidentiality.

Keywords Healthcare, Security, HIPAA, Cyber Security, Blockchain, information security,

1. Introduction

A s information technology has advanced, medical organizations have digitized their internal data, leading to the establishment of comprehensive medical information systems.. Additionally, the Internet has improved the communication of information and significantly influenced the evolution of medical information systems, enabling extensive transmission of medical data online [1]. As there is potential rise in healthcare data collected from various entities like hospital, nursing facilities, labs, pharmacies, ambulatory services, physician offices, government agencies, the centralized disintegrated nature of data become prominent challenge for healthcare industry to preserve and secure this data for several years. Some regulations demand the data should be retained for a minimum of 6 year. In this paper we will understand the history, potential and intensity of the cause, the actual cause and efforts made to safeguard from worse and uncover potential solutions available.

The overall security approach can be divided into 3 main aspects.

Administrative safeguards – This applies and encourages healthcare entities to establish regulatory, and enterprise defined administrative safeguards at their workstations, care facilities and embed them in work culture.

2. Policy creation and enforcement

Individual healthcare institutions, government bodies and interested partnership entities to create strong policies, adjust them situationally for healthcare data, fraud prevention. Drive substantial workforce to ensure the enforcement of these policies on periodic intervals, encourage renewals of these policies.

3.Cyber security protection

Implementation of measures and protocols designed to safeguard the confidentiality, integrity, and availability of healthcare information systems and data from cyber threats. Given the sensitive nature of patient data and the increasing digitization of healthcare processes, robust cybersecurity is essential to prevent unauthorized access, data breaches, and disruptions to healthcare services. By integrating cybersecurity measures, healthcare organizations aim to create a resilient and secure environment for managing patient data, supporting the delivery of healthcare services, and maintaining the trust of patients and stakeholders.

4. History and potential of data

The concept of electronic health records (EHRs) has been evolving over several decades, with efforts to digitize and modernize healthcare information systems. The transition from traditional paper-based medical records to electronic formats has been a gradual process. The growing use of cloud computing, digital devices, IoT, Smart wearables, and artificial intelligence (AI) adding more security challenges to healthcare information. Despite, having standard norms, regulations, and policies, the security of the information is still a challenge to the healthcare world. Let's look at the rise of healthcare information and security challenges first.

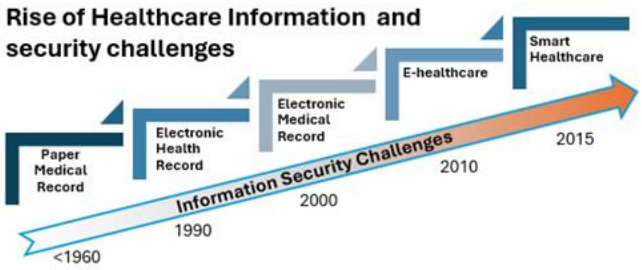

Figure 1: Rise of Healthcare information and security challenges over the period of time

Below are significant landmarks in the evolution and widespread use of electronic health records, which have consequently led to an expansion in healthcare data volume.

1960s-1970s: Early Computerized Patient Records:

The use of computers in healthcare began in the 1960s and 1970s, with the development of early computerized patient record systems. These systems were primarily used for administrative purposes and had limited clinical functionalities.

1980s: Rise of Hospital Information Systems (HIS):

Hospital Information Systems started to gain popularity in the 1980s. These systems focused on managing administrative and financial aspects of healthcare but included some clinical data.

1990s: Development of EHR Standards:

The 1990s saw the development of standards for electronic health records, with organizations such as the Institute of Medicine (IOM) advocating for the use of electronic records to improve patient care and safety.[2]

Early 2000s: Increased Adoption and Government Initiatives:

In the early 2000s, there was a increasing recognition of the potential advantages of EHRs. Initiatives such as the U.S. government's Healthcare Information Technology for Economic and Clinical Health (HITECH) Act in 2009 provided incentives for the adoption of EHRs in the United States.

Mid-2000s: Accelerated Adoption and Meaningful Use:

The mid-2000s witnessed a significant increase in the adoption of EHRs, driven by advancements in technology, government incentives, and the push for "meaningful use" of electronic health records. Healthcare organizations were incentivized to demonstrate the meaningful use of EHRs to improve patient care.

Present Day: Global Adoption and Interoperability:
EHR adoption has become widespread globally. Modern EHR systems focus on interoperability, allowing healthcare providers to share patient information seamlessly across different healthcare entities. Standardization efforts, such as the adoption of HL7 and SNOMED CT, contribute to interoperability.
The transition to EHRs continues to evolve, with ongoing efforts to address challenges related to interoperability, data security, and user experience. EHRs play a crucial role in enhancing patient care, improving data accessibility, and facilitating healthcare analytics for better decision-making. The specific timeline and milestones may vary by country and region, but the overall trend is towards the widespread adoption of electronic health records inclined toward smart healthcare.

5. The Intensity of data breach

In accordance with the HITECH Act, Section 13402(e)(4) mandates that the Secretary publish a list detailing instances where unsecured protected health information of 500 or more individuals has been compromised. All breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights can be found at U.S Department of Health and Human Services, Office for Civil Rights, here, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. There are 600+ cases open just for the year 2023. [3]

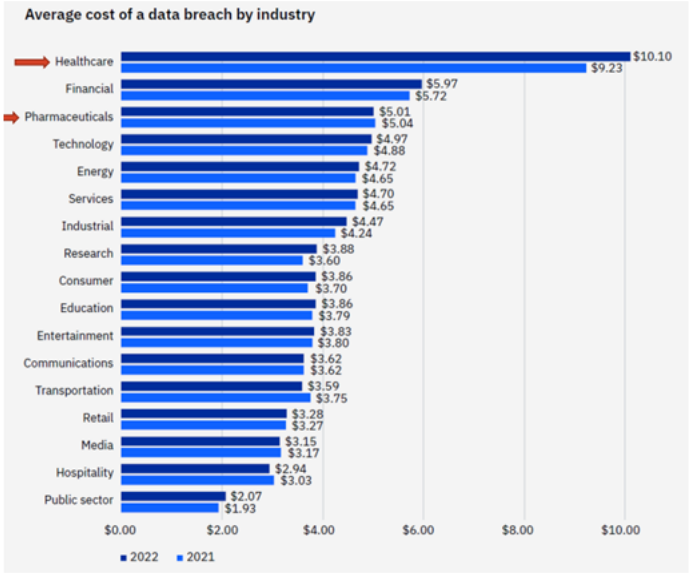

Figure. 2 Average Cost of data breach by industry, release by IBM at 2022 Healthcare Cybersecurity Year in Review, and 2023 Look-Ahead, published on February 9, 2023

For the 12th year in a row, the health sector had the highest costs for a data breach. The average breach in healthcare increased by nearly $1M and is now $10.1M. Costs have also increased over 40% in the last two years, according to the data.[3].In 2023, healthcare data breaches involving over 540 organizations and affecting more than 112 million people were reported to the HHS Office for Civil Rights (OCR), a significant increase from the 590 organizations and 48.6 million individuals affected in 2022 [4]. Servers, databases, and email continue to be heavily targeted for sensitive data. Most data breaches happened at the Business Associate locations (60%) followed by healthcare providers (30%) and health plans (10%) [4].

6. Defend the Attack

Healthcare information security is paramount for safeguarding the confidentiality, integrity, and availability of patient data. Robust security measures are essential to prevent unauthorized access to sensitive medical records, ensuring patient privacy and compliance with regulations. Healthcare organizations must adhere to strict data security regulations, such as HIPAA, to avoid legal repercussions and maintain the trust of patients. The healthcare sector faces evolving cybersecurity threats, requiring continuous efforts to identify, assess, and mitigate potential risks to patient information. Information security in healthcare focuses on maintaining the accuracy and consistency of medical records to support informed clinical decision-making. As healthcare

transitions to electronic health records, robust security protocols are crucial to protect digital patient information from cyber threats. A secure healthcare information system is foundational for building and maintaining patient trust by assuring the confidentiality of their personal and medical data. Preparedness for security incidents is key, with healthcare organizations establishing comprehensive incident response and recovery plans to minimize the impact of breaches. Ensuring secure data exchange between healthcare systems and devices is essential for achieving interoperability without compromising information security. Healthcare staff must receive regular training on security protocols and stay informed about evolving cybersecurity threats to actively contribute to the overall information security posture of the organization. Employ encryption techniques to secure data both in transit and at rest, protecting it from interception or unauthorized access. Implement strict access controls to ensure that only authorized individuals have access to sensitive healthcare information. Deploy firewalls, intrusion detection/prevention systems, and other network security measures to defend against cyber-attacks and unauthorized access. Secure devices such as computers, laptops, and medical devices to prevent malware, ransomware, and other cyber threats. Refrain from encouraging the BYOD (Bring your own device) policy if there are no surveillance mechanisms for personal devices. Develop and implement incident response plans to detect, respond to, and mitigate the impact of cybersecurity incidents promptly. Provide ongoing cybersecurity training for healthcare staff to raise awareness about potential threats and promote best practices for data security. Assess and monitor the cybersecurity practices of third-party vendors that have access to healthcare systems or data. Regularly back up healthcare data and ensure that backup systems are secure and accessible for data recovery in case of a cyber incident. Ensure the disaster recovery plan is committed to the business continuity plan. Adhere to healthcare-specific regulations, such as HIPAA (Health Insurance Portability and Accountability Act), PHI (Protected Health Information), and other relevant data protection standards. Implement continuous monitoring of networks and systems to promptly identify and respond to security threats and vulnerabilities. Continuously refresh and fix software and systems to mitigate known weaknesses and minimize the chances of being exploited and tackle vulnerabilities. Implement strong authentication methods, such as multi-factor authentication, to enhance user verification and access control. Conduct regular security audits and assessments to identify weaknesses in the cybersecurity infrastructure and address them proactively.
Moreover, the importance of ethics and a code of conduct in every day's practice is of utmost importance to minimize data threats.

7. Is blockchain a solution

Blockchain technology has the potential to enhance cybersecurity in healthcare and address specific challenges related to data security and integrity. Blockchain technology represents a secure, transparent, and immutable distributed ledger system that records transactions across a network of computers in a decentralized fashion. The fundamental concept of blockchain technology gives a basis for cooperation between unknown and untrustworthy things, while also corroborating the disseminated features of mobile (smart health) devices, lacking the need for a central security and authentication authority, as in the current cloud computing architectures [5]. This main technology relies on an immutable "public ledger", which is a record of data shared among all the participants. This public ledger contains blocks of data, linked to get her with the use of a cryptographic hash key. The linking process (also known as consensus) is called Proof of Work (PoW)[6].
Both the ledger and the consensus mechanism are innately impervious to data manipulation. The block data cannot be altered post-fact because this invalidates previous block hashes in the blockchain and breaks the consensus among nodes. The key characteristics of blockchain technology include decentralized control, data transparency and auditability, distributed information, and security from malicious actors [5][6].
Blockchain can be used in EHR, consent management, Supply chain, Clinical trial research, cyber security, health payment and billing, credentialing and verification.

8. Conclusion

In conclusion, healthcare security is a critical and evolving aspect of the healthcare industry, essential for safeguarding patient data, maintaining trust, and ensuring the integrity of healthcare systems. The increasing digitization of health records, adoption of electronic health records (EHRs), and integration of emerging technologies demand robust cybersecurity measures. Protection against unauthorized access, data breaches, and

cyber threats is imperative to uphold patient privacy, comply with regulations, and sustain operational continuity.

Healthcare organizations must prioritize continuous training for staff, implement stringent access controls, and stay abreast of evolving cybersecurity threats. Additionally, advancements in technologies like blockchain hold promise in fortifying data security, enhancing transparency, and promoting patient-centric control over health information.

As the healthcare landscape continues to evolve, a proactive and comprehensive approach to cybersecurity is essential. Collaboration across stakeholders, adherence to regulatory standards, and the integration of innovative solutions will be key to fostering a secure healthcare environment. Ultimately, the goal is to strike a balance between technological innovation and robust security practices to ensure that patient information remains confidential, healthcare systems remain resilient, and the trust of patients and stakeholders is preserved.

9. Appendix

PHI - Protected Health Information

HIPAA– Health Insurance Portability and Accountability Act

SNOMED- Systematized Nomenclature of Medicine Clinical Terms (CT). Represents coded terms that may be used within EHRs to capture, record, and share clinical data for use in healthcare organizations.

EHR- Electronic Health Record

EMR – Electronic Medical Record

HITECH - Health Information Technology for Economic and Clinical Health Act. The American Recovery & Reinvestment Act of 2009 (ARRA, or Recovery Act), established the Health Information Technology for Economic Clinical Health Act (HITECH Act), which requires that CMS provide incentive payments under Medicare and Medicaid to “Meaningful Users” of Electronic Health Records

References

[1]. Chia-Hui Liu, Yu-Fang Chung, Tzer-Shyong Chen & Sheng-De Wang, C 2012, The Enhancement of Security in Healthcare Information Systems, Vol 36, Pages1673-1688

[2]. IOM Global Appeal, Retrieved from https://www.iom.int

[3]. Office of Information Security, “2022 Healthcare Cybersecurity year in Review, and a 2023 Look-Ahead, Year 2023, Retrieved From https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

[4]. Health IT Security - This Year’s Largest Healthcare Data Breaches. Retrieved from https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches

[5]. T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems, IEEE Transactions on Knowledge and Data Engineering 30 (7) (2018) 1366–1385.

[6]. U. Khalid, M. Asim, T. Baker, P.C. Hung, M.A. Tariq, L. Rafferty, A decentralized light weight block chain-based authentication mechanism for iot systems, Cluster Computing (2020)1–21.

[7]. F. T. Jaigirdar, C. Rudolph, C. Bain, Can i trust the data i see? a physician’s concern on medical data in iot health architectures, in: Proceedings of the Australasian Computer Science Week Multiconference, 2019, pp. 1–10.

[8]. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. E-Healthcare System Using Blockchain for Secure EHRs Sharing of Mobile Cloud Based with Machine Learning. Int. J. Sci. Dev. Res. 2020, 5, 66792–66806. [Google Scholar]

[9]. Al Ghamdi, D., Madini O. Alassafi, Abdulrahman A. Alshdadi, Mohamed M. Dessouky, Rabie A. Ramdan, Bassam W. Aboshosha. (2022, December 23). Developing Trusted IoT Healthcare Information-Based AI and Blockchain. Retrieved from https://www.mdpi.com/2227-9717/11/1/34.

[10]. Vijay A, A. (2023, December 10). Safeguarding the Digital Realm: The Indispensable Role of Cybersecurity in Securing Data and Technology. Retrieved from

[11]. Admin, A. (2023, October 11). trendzguruji.me awareness Of Cyber Security - Digital Journal USA. Retrieved from https://www.digitaljournalusa.com/2023/10/11/trendzguruji-me-awareness-of-cyber-security/

[12]. Sharma, P.; Moparthi, N.; Namasudra, S.; Shanmuganathan, V.; Hsu, C. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. Expert Syst. 2020, 39, e12915.

About Author:

Santosh S Deshmukh. The author is a seasoned IT professional, with an illustrative career of over two decades in Information Technology (IT) and a profound wealth of knowledge in the US healthcare landscape. The author is an independent researcher, specialized in developing cutting-edge products, security implementation and large-scale health systems. The Author is 48 years old and a current resident of McKinney, North Texas. The Author earned a master's degree in Business Analytics from Grand Canyon University, Phoenix, AZ in 2020. His fields of study are Computer science, Business Analytics and Healthcare.

He worked as Sr. PROJECT CONSULTANT (IT) for esteemed organizations like United Health, Blue Cross Blue Shield, CVS, Emblem Health, and General Motors. Currently, he has been working as a Project Consultant for Anthem Inc. since 2019. For the past 15 years, he has been at the forefront of managing complex healthcare IT initiatives, demonstrating a keen understanding of the dynamic and regulated healthcare environment. With a significant focus on Healthcare Analytics, he has seamlessly integrated his knowledge to address the unique challenges within the healthcare sector, contributing to the improvement of patient outcomes and operational efficiency.

Mr. Deshmukh is a certified Project Management Professional (PMP) since 2009. Mr. Deshmukh is an expert professional with a unique blend of technical acumen, project management expertise, and a significant impact on the U.S. healthcare system. Besides, Mr. Deshmukh is also a lifetime member of Sigma Beta Delta (SBD). An honorary member of IEEE since 2020 and Sr. Member since 2021. Mr. Deshmukh is also a member of the Advisory Board of Our Lady of the Lake University, Houston. Mr. Deshmukh served in a secretary position at a non-profit organization during 2022-23. Author email id is san_desh3@yahoo.com.