iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62199

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

The Future of Patient Data Security: Exploring Emerging Technologies and Collaborative Approaches

Naga Vinod Duggirala
Andhra University, INDIA

Abstract: ***The protection of sensitive patient data has become a paramount concern in the increasingly digital landscape of the healthcare industry. As healthcare organizations adopt electronic health records and face a growing array of cyber threats, they must navigate a complex regulatory environment, including the Health Insurance Portability and Accountability Act (HIPAA), while implementing robust strategies to safeguard personal health information (PHI). This article provides a comprehensive overview of the challenges and best practices in healthcare data protection, examining the current regulatory framework, the various threats to patient data—such as cyber-attacks, insider threats, and human error—and the key strategies and technologies for enhancing security, including encryption, access controls, and employee training. The article also explores the potential of emerging technologies, such as block chain and artificial intelligence, in revolutionizing healthcare data management and security, and emphasizes the importance of collaboration among stakeholders, including healthcare providers, technology vendors, policymakers, and patients. By recapping the main challenges and strategies discussed, offering insights into the future of data protection in healthcare, and issuing a call to action for prioritizing patient data security, this article serves as a valuable resource for healthcare organizations seeking to strengthen their data protection measures and maintain patient trust in the digital age.***

Keywords: Patient Data Security, Healthcare Data Protection, Emerging Technologies, Regulatory Compliance, Collaboration in Healthcare



I. INTRODUCTION

In today's increasingly digital healthcare landscape, the protection of sensitive patient data has become a paramount concern for healthcare providers, policymakers, and patients alike. As the industry continues to embrace technological advancements and the adoption of electronic health records (EHRs), the risk of data breaches and unauthorized access to personal health information (PHI) has escalated significantly [1]. According to a report by the Healthcare Information and Management Systems Society (HIMSS), healthcare data breaches have affected over 189 million records in the United States since 2009 [2], underscoring the urgent need for robust data protection strategies.

©IJRASET: All Rights are Reserved

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 laid the foundation for safeguarding patient data privacy and security in the United States [3].

However, as technology continues to evolve and cyber threats become more sophisticated, healthcare organizations must go beyond basic HIPAA compliance to ensure the confidentiality, integrity, and availability of patient data [4]. The consequences of non-compliance and data breaches extend far beyond financial penalties, as they can erode patient trust, damage an organization's reputation, and hinder the quality of patient care [5].

A study by the Ponemon Institute revealed that the average cost of a healthcare data breach reached $7.13 million in 2020, marking a 10.5% increase from the previous year [6]. Moreover, the healthcare industry faces unique challenges in protecting sensitive data due to the complex network of stakeholders involved, including healthcare providers, insurance companies, pharmacies, and medical device manufacturers [7].

As a result, safeguarding patient data requires a multi-faceted approach that encompasses regulatory compliance, technological solutions, employee training, and ongoing risk assessment [8].

This article aims to explore the critical challenges faced by the healthcare industry in protecting sensitive patient data and discuss the strategies and best practices for ensuring data privacy and security. By examining the current regulatory landscape, prevalent threats, and emerging technologies, we hope to provide valuable insights for healthcare organizations seeking to strengthen their data protection measures and maintain patient trust in the digital age.

II. REGULATORY COMPLIANCE

A. Overview of HIPAA Regulations

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to protect sensitive patient health information from being disclosed without the patient's consent or knowledge [9]. HIPAA's Privacy Rule and Security Rule establish national standards for the protection of PHI, including electronic PHI (ePHI) [10]. The Privacy Rule sets limits on the use and disclosure of PHI, while the Security Rule outlines the technical, physical, and administrative safeguards required to ensure the confidentiality, integrity, and availability of ePHI [11].

B. Consequences Of Non-Compliance

Non-compliance with HIPAA regulations can result in significant financial penalties and reputational damage for healthcare organizations. The Department of Health and Human Services' Office for Civil Rights (OCR) is responsible for enforcing HIPAA rules and can impose fines ranging from $100 to $50,000 per violation, with an annual maximum of $1.5 million for repeat violations [12]. In addition to financial penalties, non-compliance can lead to criminal charges, lawsuits, and loss of patient trust [13].

C. Other Relevant Regulations And Standards

In addition to HIPAA, healthcare organizations must comply with various other regulations and standards related to data protection. The Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that process credit card payments, while the General Data Protection Regulation (GDPR) affects healthcare providers that treat patients from the European Union [14]. The National Institute of Standards and Technology (NIST) also provides guidelines for safeguarding PHI, such as the NIST Cybersecurity Framework and NIST SP 800-66 [15].

III. THREATS TO PATIENT DATA

A. Cyber Attacks

1) Types Of Cyber Threats

Healthcare organizations face a wide range of cyber threats, including malware, phishing, ransomware, and denial-of-service attacks [16]. Malware, such as viruses and Trojans, can infiltrate healthcare systems and steal sensitive data, while phishing attacks trick employees into revealing login credentials or installing malicious software [17]. Ransomware attacks encrypt an organization's data and demand payment in exchange for the decryption key, disrupting patient care and potentially exposing PHI [18].

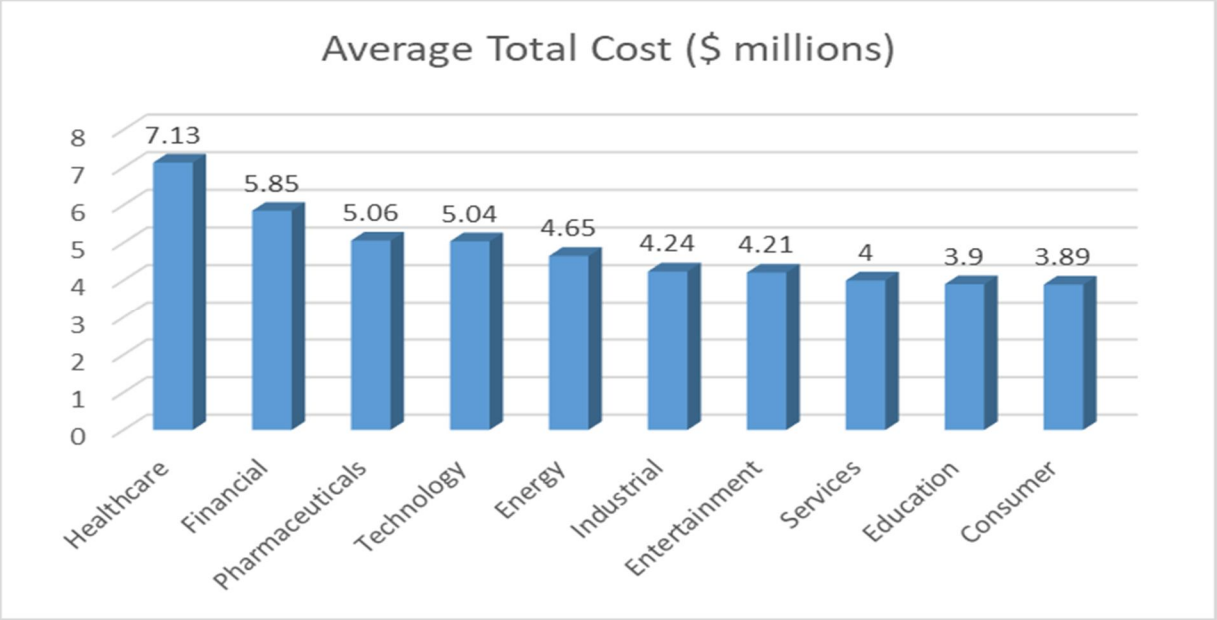


Table 1: Healthcare Data Breach Costs by Industry Sector [19][20]

B. Insider Threats

1) Intentional Misuse Of Data By Employees

Insider threats, which involve the misuse of data by employees or other authorized individuals, pose a significant risk to patient data security. In a 2019 survey by Verizon, 59% of healthcare data breaches were caused by insiders [21]. Insider threats can be motivated by financial gain, personal disputes, or negligence [22].

2) Accidental Data Exposure By Staff

Accidental data exposure by staff, such as sending PHI to the wrong recipient or losing a laptop containing unencrypted patient data, can also lead to significant data breaches. A study by Ponemon Institute found that 62% of insider-related incidents in healthcare were due to employee negligence [23].

C. Human Error

1) Mishandling Of Sensitive Information

Human error, such as the mishandling of sensitive information, is a major contributor to data breaches in healthcare. Examples include improperly disposing of paper records containing PHI, leaving computer screens with PHI visible in public areas, and sharing login credentials with unauthorized individuals [24].

2) Importance Of Proper Data Management Practices

Proper data management practices, such as implementing access controls, regularly training employees, and maintaining an inventory of all devices containing PHI, are essential for minimizing the risk of human error [25]. Healthcare organizations should also have clear policies and procedures in place for handling and disposing of sensitive information [26].

D. Data Protection Strategies And Technologies

Strategy/Technology	Description	Benefits
Encryption	Encoding data to prevent unauthorized access	Protects data at rest and in transit
Access Controls	Restricting data access based on user roles and permissions	Prevents unauthorized data access
Employee Training	Educating staff on data protection best	Reduces human error and insider

Strategy/Technology	Description	Benefits
	practices	threats
Data Loss Prevention	Monitoring and blocking potential data leaks	Prevents accidental or malicious data loss
Network Segmentation	Separating sensitive data from less critical systems	Limits the impact of a breach
Intrusion Detection/Prevention	Monitoring and blocking malicious network activity	Detects and prevents cyber attacks
Multi-Factor Authentication	Requiring multiple forms of authentication	Enhances access control and prevents unauthorized login
Regular Risk Assessments	Identifying and addressing potential vulnerabilities	Proactively mitigates risks
Incident Response Planning	Establishing procedures for handling data breaches	Minimizes damage and ensures prompt response
Third-Party Risk Management	Assessing and monitoring vendor security practices	Reduces risks from third-party vulnerabilities

Table 1: Key Data Protection Strategies and Technologies in Healthcare [27-38]

E. Encryption

1) Role Of Encryption In Securing Patient Data

Encryption is a critical tool for securing patient data, as it renders PHI unreadable to unauthorized individuals [27]. By encrypting data at rest and in transit, healthcare organizations can significantly reduce the risk of data breaches and ensure compliance with HIPAA regulations [28].

2) Types Of Encryption Used In Healthcare

Healthcare organizations typically use symmetric and asymmetric encryption algorithms to protect PHI. Symmetric encryption, such as Advanced Encryption Standard (AES), uses the same key for both encryption and decryption, while asymmetric encryption, like Rivest-Shamir-Adleman (RSA), uses a public key for encryption and a private key for decryption [29]. Other encryption technologies used in healthcare include full-disk encryption, file-level encryption, and email encryption [30].

F. Access Controls

1) Importance Of Limiting Access To Sensitive Data

Limiting access to sensitive data is a fundamental principle of data security in healthcare. By implementing access controls, organizations can ensure that only authorized individuals can view, modify, or transmit PHI [31]. This reduces the risk of insider threats and accidental data exposure [32].

2) Implementing Role-Based Access Controls

Role-based access controls (RBAC) are a common method for managing access to PHI in healthcare organizations. RBAC assigns permissions to users based on their roles and responsibilities within the organization, ensuring that individuals only have access to the data necessary for their job functions [33]. This approach simplifies access management and enhances security by minimizing the potential for unauthorized access [34].

IV. EMPLOYEE TRAINING AND AWARENESS

1) Educating Staff On Data Protection Best Practices

Employee training and awareness are essential components of data protection in healthcare. By educating staff on data protection best practices, such as creating strong passwords, identifying phishing emails, and properly handling PHI, organizations can reduce the risk of human error and insider threats [35]. Training should be conducted regularly and updated to address emerging threats and changes in regulations [36].

2) Regularly Updating Training Programs

Healthcare organizations should regularly update their training programs to ensure that employees are aware of the latest data protection best practices and regulatory requirements. This can include annual HIPAA training, cybersecurity awareness training, and job-specific training for roles that involve handling sensitive data [37]. Organizations should also consider implementing phishing simulations and other hands-on exercises to reinforce training concepts [38].

V. EMERGING TECHNOLOGIES IN HEALTHCARE DATA PROTECTION

A. Blockchain

1) Potential Applications of Blockchain in Healthcare Data Management

Blockchain technology has the potential to revolutionize healthcare data management by providing a secure, decentralized platform for storing and sharing PHI [39]. By using blockchain, healthcare organizations can create an immutable record of all transactions involving PHI, enhancing data integrity and preventing unauthorized modifications [40]. Blockchain can also facilitate secure data sharing between healthcare providers, researchers, and patients, enabling more efficient and effective care delivery [41].

2) Challenges and Limitations of Implementing Blockchain Solutions

Despite the potential benefits of blockchain in healthcare, several challenges and limitations must be addressed before widespread adoption can occur. These include scalability issues, high energy consumption, lack of standardization, and regulatory uncertainties [42]. Additionally, implementing blockchain solutions requires significant investment in infrastructure and workforce training [43].

B. Artificial Intelligence

1) Using AI for Anomaly Detection and threat Prevention

Artificial intelligence (AI) can play a crucial role in enhancing healthcare data security by enabling real-time anomaly detection and threat prevention [44]. Machine learning algorithms can analyze large volumes of data to identify unusual patterns and potential security incidents, such as unauthorized access attempts or data exfiltration [45]. AI-powered tools can also help automate security tasks, such as patch management and vulnerability assessments, freeing up IT staff to focus on more strategic initiatives [46].

2) Ethical Considerations Surrounding AI in Healthcare

While AI offers significant benefits for healthcare data protection, it also raises important ethical considerations. These include concerns around bias and discrimination in AI algorithms, the potential for AI to be used for malicious purposes, and the impact of AI on patient privacy and autonomy [47]. Healthcare organizations must ensure that AI systems are transparent, accountable, and aligned with ethical principles to maintain patient trust and safeguard sensitive data [48].

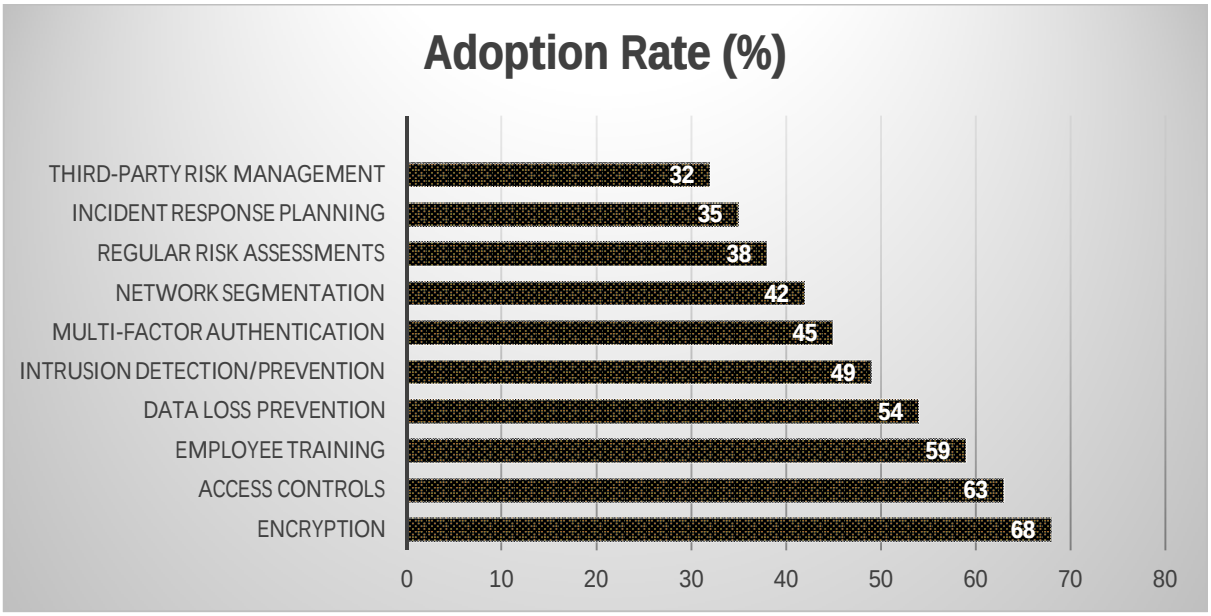


Figure 2: Adoption Rates of Key Data Protection Technologies in Healthcare[55]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

VI. COLLABORATION AND STAKEHOLDER ENGAGEMENT

A. Importance of collaboration between healthcare providers and technology vendors

Collaboration between healthcare providers and technology vendors is essential for effective data protection in the healthcare industry. By working together, these stakeholders can develop and implement comprehensive security solutions that address the unique challenges of protecting PHI [49]. Technology vendors can provide expertise in areas such as encryption, access controls, and threat detection, while healthcare providers can offer valuable insights into the operational and clinical aspects of data protection [50].

B. Role of Policymakers in Shaping Data Protection Regulations

Policymakers play a critical role in shaping data protection regulations in the healthcare industry. By enacting laws and guidelines, such as HIPAA and the NIST Cybersecurity Framework, policymakers establish the legal and regulatory framework for safeguarding PHI [51]. As technology and cyber threats continue to evolve, policymakers must work closely with healthcare providers, technology vendors, and other stakeholders to update and refine data protection regulations to ensure they remain effective and relevant [52].

Regulation	Jurisdiction	Key Requirements	Penalties
HIPAA (Health Insurance Portability and Accountability Act)	United States	• Protected Health Information (PHI) must be kept secure and confidential Covered entities must implement appropriate administrative, physical, and technical safeguards • Patients have the right to access and request corrections to their PHI	• Fines up to $50,000 per violation, with an annual maximum of $1.5 million • Possible criminal charges for willful neglect
GDPR (General Data Protection Regulation)	European Union	• Personal data must be processed lawfully, fairly, and transparently • Data controllers must obtain explicit consent for data processing • Data subjects have the right to access, rectify, erase, and restrict processing of their personal data • Data breaches must be reported within 72 hours	Fines up to €20 million or 4% of global annual turnover, whichever is higher
CCPA (California Consumer Privacy Act)	California, United States	• Consumers have the right to know what personal information is being collected, sold, or disclosed • Consumers can opt-out of the sale of their personal information • Businesses must implement reasonable security measures to protect consumer data	• Fines up to $7,500 per intentional violation • Consumers can sue for damages in the event of a data breach

Table 2: Comparison of Data Protection Regulations in the United States and European Union [56-61]

This table compares three major data protection regulations: HIPAA in the United States, GDPR in the European Union, and CCPA in California. It highlights the key requirements, penalties, and jurisdictions of each regulation.

©IJRASET: All Rights are Reserved

C. Engaging Patients in the data Protection Process

Engaging patients in the data protection process is crucial for building trust and ensuring the success of data security initiatives in healthcare. By educating patients about their rights under HIPAA and other regulations, healthcare organizations can empower them to make informed decisions about the use and disclosure of their PHI [53]. Healthcare providers should also be transparent about their data protection practices and provide patients with clear mechanisms for accessing, correcting, and controlling their personal health information [54].

VII. CONCLUSION

Protecting sensitive patient data in the healthcare industry is a complex and ongoing challenge. Healthcare organizations must navigate a myriad of threats, including cyber-attacks, insider threats, and human error, while complying with a growing array of regulations and standards. To effectively safeguard PHI, healthcare providers must implement a comprehensive data protection strategy that encompasses encryption, access controls, employee training, and collaboration with key stakeholders. As technology continues to advance and cyber threats become more sophisticated, the future of data protection in the healthcare industry will require ongoing innovation and adaptation. Emerging technologies, such as blockchain and AI, offer promising solutions for enhancing data security and enabling secure data sharing. However, these technologies also present new challenges and ethical considerations that must be carefully addressed.

Ultimately, protecting sensitive patient data must be a top priority for everyone involved in the healthcare industry. Healthcare providers, technology vendors, policymakers, and patients all have a role to play in ensuring the privacy and security of PHI. By working together and investing in robust data protection measures, we can create a healthcare system that delivers high-quality, personalized care while safeguarding the trust and privacy of patients.

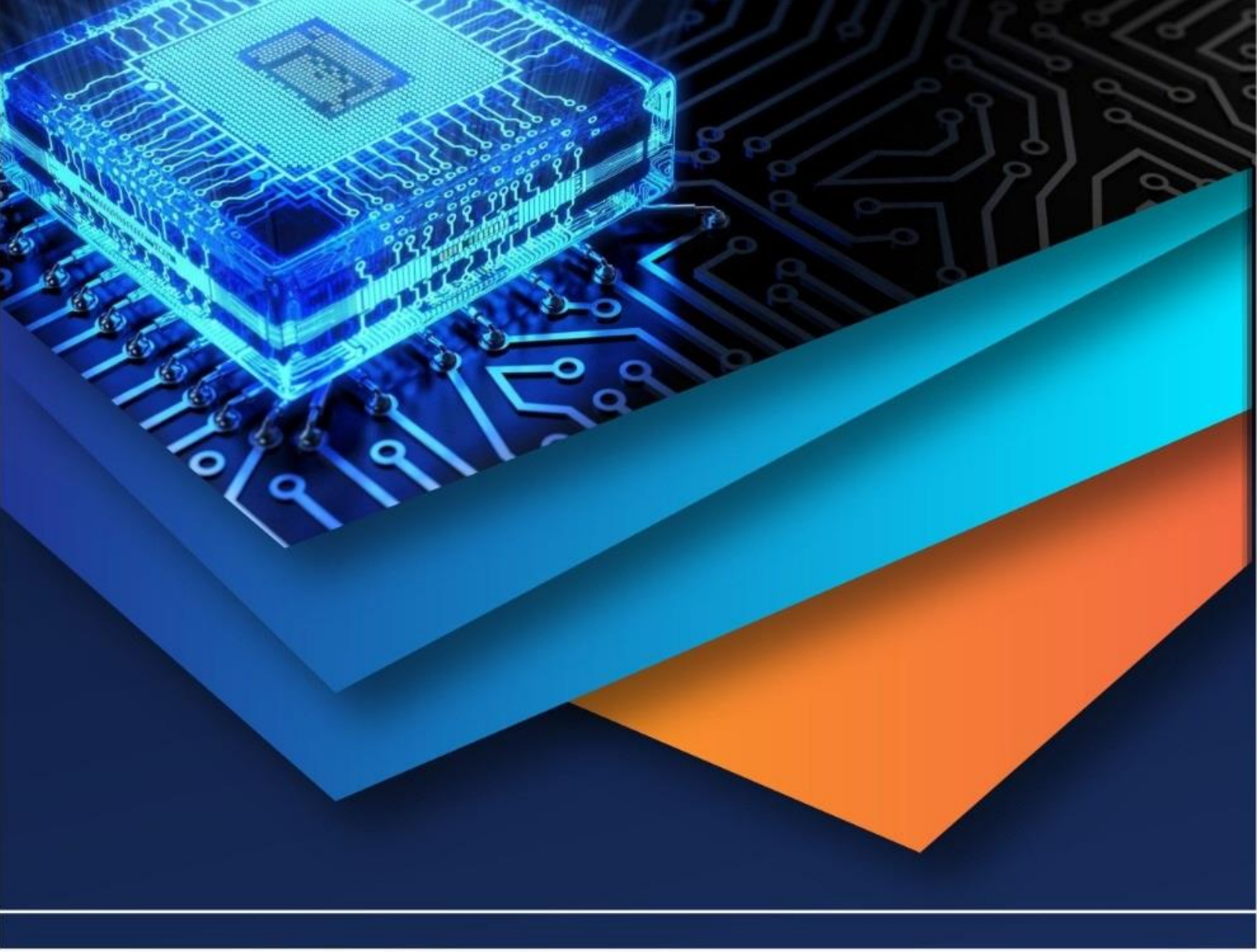
REFERENCES

[1] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48-52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.
[2] Healthcare Information and Management Systems Society (HIMSS), "2021 HIMSS Healthcare Cybersecurity Survey," HIMSS, 2021, [Online]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey.
[3] U.S. Department of Health and Human Services, "The HIPAA Privacy Rule," HHS.gov, 2021, [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
[4] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health Care and Cybersecurity: Bibliometric Analysis of the Literature," J Med Internet Res, vol. 21, no. 2, p. e12644, Feb. 2019, doi: 10.2196/12644.
[5] P. J. Wagner and M. D. Wernert, "The Impact of Data Breaches on Brand Reputation and Trust in the Healthcare Industry," J Healthc Qual, vol. 41, no. 1, pp. 15-23, Jan. 2019, doi: 10.1097/JHQ.0000000000000147.
[6] Ponemon Institute, "Cost of a Data Breach Report 2020," Ponemon Institute, 2020, [Online]. Available: https://www.ibm.com/security/data-breach.
[7] S. S. Rao and D. M. Rao, "Addressing Cyber Security Challenges in Healthcare," Int J E-Health Med Commun, vol. 12, no. 2, pp. 1-18, Apr. 2021, doi: 10.4018/IJEHMC.2021040101.
[8] M. Niazi, S. Ikram, and M. Bano, "A Comprehensive Review on Cybersecurity and Data Privacy in Healthcare," Sensors (Basel), vol. 21, no. 20, p. 6810, Oct. 2021, doi: 10.3390/s21206810.
[9] U.S. Department of Health and Human Services. (2013). HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
[10] U.S. Department of Health and Human Services. (2017). HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/index.html
[11] Agris, J. (2014). Extending the HIPAA Privacy Rule to Personal Health Records. Journal of AHIMA, 85(4), 50-53.
[12] Solove, D. J. (2013). HIPAA Turns 10: Analyzing the Past, Present, and Future Impact. Journal of AHIMA, 84(4), 22-28.
[13] Wikina, S. B. (2014). What caused the breach? An examination of the use of information technology and health data breaches. Perspectives in Health Information Management, 11(Fall), 1h.
[14] Pillay, M. (2020). Data protection in healthcare: A review of the current landscape. South African Journal of Bioethics and Law, 13(2), 50-55. https://doi.org/10.7196/SAJBL.2020.v13i2.727
[15] Karamanian, A. (2019). Revisiting HIPAA and NIST guidelines for healthcare cybersecurity. Journal of Healthcare Protection Management, 35(1), 52-59.
[16] Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008
[17] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10. https://doi.org/10.3233/THC-161263
[18] Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied Clinical Informatics, 7(2), 624-632. https://doi.org/10.4338/ACI-2016-04-SOA-0064
[19] Wee, C. (2021). Scripps Health cyberattack: What we know. MedCity News. https://medcitynews.com/2021/05/scripps-health-cyberattack-what-we-know/
[20] Davis, J. (2019). AMCA breach impact reaches 20 million as more labs report. Health IT Security. https://healthitsecurity.com/news/amca-breach-impact-reaches-20-million-as-more-labs-report

[21] Verizon. (2019). 2019 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[22] Markel Foundation & Databreaches.net. (2021). Insider threats in healthcare: A study of user behaviors that can introduce risk. https://markel-foundation.com/wp-content/uploads/2021/09/Insider-Threats-in-Healthcare-Report-2021.pdf
[23] Ponemon Institute. (2020). 2020 Cost of Insider Threats: Global Report. https://www.observeit.com/cost-of-insider-threats/
[24] Vaidya, A. (2019). Human errors in healthcare data breaches. Journal of AHIMA, 90(4), 36-39.
[25] U.S. Department of Health and Human Services. (2017). HIPAA Security Rule: Guidance on Risk Analysis. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[26] AHIMA. (2018). Disposal of Protected Health Information. https://journal.ahima.org/disposal-of-protected-health-information/
[27] Faezi, S., Louie, D., Seltzer, A., & Haydel, M. (2019). Encryption in healthcare: A primer. Journal of AHIMA, 90(5), 18-23.
[28] Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. ACM Computing Surveys, 45(1), 1-54. https://doi.org/10.1145/2379776.237977
[29] Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal, 19(4), 439-444. https://doi.org/10.5829/idosi.wasj.2012.19.04.1837
[30] Hou, S., Ye, Y., Song, Y., & Abdulhayoglu, M. (2017). Hindroid: An intelligent Android malware detection system based on structured heterogeneous information network. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1507-1515. https://doi.org/10.1145/3097983.3098026
[31] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541-562. https://doi.org/10.1016/j.jbi.2012.12.003
[32] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management, 6(4), 279-314. https://doi.org/10.1504/IJIEM.2010.035624
[33] Chen, X., & Zheng, Q. (2012). A security architecture for access control of personal health information. Proceedings of the 2nd International Conference on Biomedical Engineering and Technology, 34, 56-60. https://doi.org/10.7763/IPCBEE.2012.V34.12
[34] Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. JAMA, 313(14), 1471-1473. https://doi.org/10.1001/jama.2015.2252
[35] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003
[36] Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The utility of information security training and education on cybersecurity incidents: Empirical evidence. Information Systems Frontiers, 21(5), 1037-1044. https://doi.org/10.1007/s10796-019-09908-y
[37] Pullin, D. W. (2018). Cybersecurity training and education: A holistic approach. Journal of Applied Security Research, 13(4), 429-441. https://doi.org/10.1080/19361610.2018.1502511
[38] Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., Landman, A. B. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Network Open, 2(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393
[39] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056
[40] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068
[41] Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating trust and interoperability. Computational and Structural Biotechnology Journal, 16, 224-230. https://doi.org/10.1016/j.csbj.2018.06.003
[42] Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1-3. https://doi.org/10.1109/HealthCom.2016.7749510
[43] Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470. https://doi.org/10.3390/sym10100470
[44] Chatterjee, P., Cymberknop, L. J., & Armentano, R. L. (2017). IoT-based decision support system for intelligent healthcare—applied to cardiovascular diseases. 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), 362-366. https://doi.org/10.1109/CSNT.2017.8418568
[45] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. Health Information Science and Systems, 2(1), 3. https://doi.org/10.1186/2047-2501-2-3
[46] Dutta, P., Dutta, P., & Sil, J. (2017). Automatic speech recognition based smart home using fuzzy logic. 2017 IEEE Calcutta Conference (CALCON), 64-67. https://doi.org/10.1109/CALCON.2017.8280682
[47] Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care—addressing ethical challenges. The New England Journal of Medicine, 378(11), 981-983. https://doi.org/10.1056/NEJMp1714229
[48] Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. PLoS Medicine, 15(11), e1002689. https://doi.org/10.1371/journal.pmed.1002689
[49] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? BMJ, 358, j3179. https://doi.org/10.1136/bmj.j3179
[50] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059
[51] Hoffman, S., & Podgurski, A. (2013). The use and misuse of biomedical data: Is bigger really better? American Journal of Law & Medicine, 39(4), 497-538. https://doi.org/10.1177/009885881303900401
[52] Terry, N. P. (2017). Regulatory disruption and arbitrage in health-care data protection. Yale Journal of Health Policy, Law, and Ethics, 17(1), 143-207.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[53] Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. JAMA, 320(3), 231-232. https://doi.org/10.1001/jama.2018.5630
[54] Enaizan, O., Zaidan, A. A., Alwi, N. H. M., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., & Albahri, A. S. (2020). Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Health and Technology, 10(3), 795-822. https://doi.org/10.1007/s12553-018-0278-7
[55] Healthcare Information and Management Systems Society (HIMSS). (2020). 2020 HIMSS Cybersecurity Survey. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
[56] U.S. Department of Health and Human Services. (2013). Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
[57] U.S. Department of Health and Human Services. (2017). HIPAA Enforcement. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html
[58] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[59] European Commission. (2021). GDPR Enforcement Tracker. https://www.enforcementtracker.com/
[60] California State Legislature. (2018). California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[61] California Office of the Attorney General. (2021). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)