ISSN: 2249-7196
IJMRR/July. 2021/ Volume 11/Issue 3/87-98
Sahil bucha / International Journal of Management Research & Review

Designing A Hipaa-Compliant Delivery System: A Framework For Secure And Efficient Healthcare Data Exchange

Author Name: **Sahil bucha**
Affiliation: Independent Ecommerce integration expert
Address:29 N tompkins sq, Downingtown,PA-19335
Email: sahilbucha@gmail.com

Abstract

This research established a detailed review of HIPAA-Compliant Delivery system support in healthcare treatment and operations. The beneficial values of AI and IoT-Driven delivery systems have been convenient to operate the healthcare mobility and operational functions in business. The competencies of security and effective data exchanging operations of HIPAA-complaints are responsible for better service maintenance in business. The complementary solutions of the delivery system allow a better transition of business movement and healthcare convenience for data recording and tracking capabilities.

Keywords: HIPAA-Compliant Delivery system, Secure and efficient healthcare, data exchange, data recording and tracking, AI and IoT-Driven delivery systems, Service maintenance, HIPAA software

I INTRODUCTION

A. Background of the Study

A comparative study on the "Health Insurance Portability and Accountability Act (HIPAA)" delivery system utilises a dynamics of security and data transferable strategy in healthcare. The illustrative study emphasises the prevalence and beneficial importance of the HIPAA delivery system in healthcare. The global market expansion rate has increased to $690.38 million market share in the healthcare industry [13]. The future extension of using the HIPAA system will increase up to 13.4% of the CAGR between 2021 and 2025.

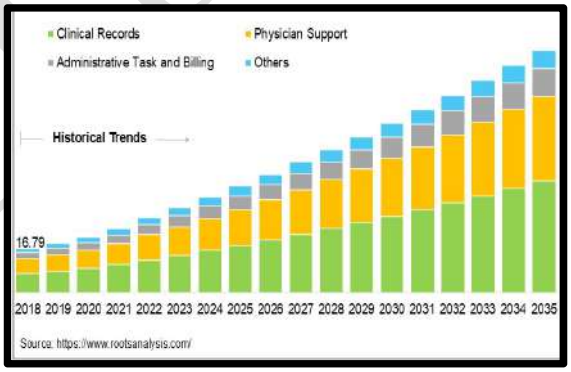

Figure 1: Global Electronic Record Market in Healthcare Industry

(Source: [1])

The usage of information sharing and data exchange supports is conjugated using the proper handling techniques of the HIPAA system. The delivery methods of complaining and feedback analysis have been considered to protect patients and market forecasts for the healthcare industry. The phase of HIPAA software work considered major components of "logging, monitoring, data backup, PHI for marketing, communication and recovery systems" for

the development of the healthcare movement [14]. The core element supports "256-bit AES Encryption" standards to allow security and data protection in the balance of operational mobility. The conditions of patient security and data controlling operations support better databases in the professional area of the healthcare industry.

B. Overview

The overview of this research paper proposes a solution of healthcare data exchange solutions introducing the generalisation and convenience in patient security management. The complementary installation of the HIPAA-Delivery system for convenient support to the security and data exchange operations is found in the healthcare industry [11]. Digitalisation and monitoring are two major factors entitled to patient care treatment to enhance the conditions and solutions for customer protection. Data recording and complementary security to online communication will be imposed using this HIPAA-delivery system in recent times.

C. Problem Statement

In this era of digitalisation, virtual communication is an exceptional practice to be entitled within the data recording and healthcare operations in recent times. The complementary practice of digital security in healthcare data tracking is a current trend. The challenges of data tracking and misleading processes are inconvenient to organising sustainable healthcare management. Focusing on the HIPAA-Delivery system supports digital technology to eliminate the potential issues of data security issues and functional disparities within social operations [15]. The patient's care and convenience in easy data recording practice is the main problem statement of this segment.

D. Objectives

- To investigate the current trends of the HIPAA-Delivery System in Healthcare data exchange processing systems.
- To analyse the beneficial advantages of the HIPAA-Delivery system in healthcare security and data exchange activities.
- To investigate the current challenges of the HIPAA-delivery system in healthcare data exchange.
- To execute the best solutions of HIPAA-Delivery System in healthcare data management scenario

E. Scope and Significance

The possible scope of this research will extend the usage of the HIPAA-Delivery system in the support of healthcare management practices and developing convenience. The information-sharing activities and functional mobility are two effective areas of this study. The cultivation of research work on HIPAA security configuration major disputes will also be identified to organize the best possible solutions for the healthcare industry using the HIPAA-Delivery Data exchange system.

II. LITERATURE REVIEW

A. HIPAA-compliant Delivery System in Healthcare Data Exchange

The healthcare industry is shifting towards digitalisation including software-driven communication and data-tracking processes. The conventional adjustment of the "Health Insurance Portability and Accountability Act (HIPAA)" is the latest regulation assembled within the healthcare industry. The importance of the HIPAA-Delivery System is a convenient part of raising digital communication and data recording practices. Patient care support from unauthorised data access is the main support of the HIPAA system in data exchange [16]. The security from digital attacks and contemporary solutions of operational support is quite convenient to utilize the

HIPAA system in information sharing practice. It has been outlined that a total of $1.77 billion market share with a transition of 11.2% of CAGR has been increased globally.

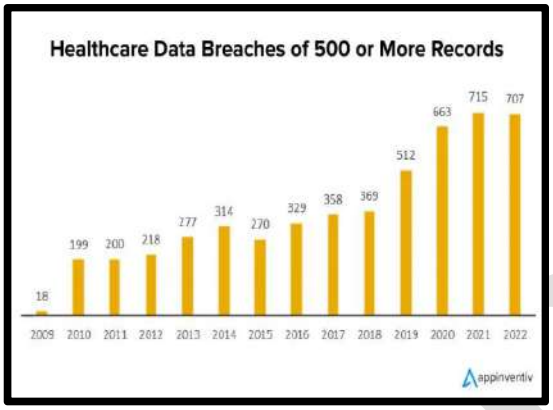

Figure 2: Healthcare Industry HIPAA Delivery Prevalence Growth

(Source: [2])

A total growth rate of $707.12 million in revenue of HIPAA-Delivery software is an easy convenient part of developing operational production. The implementation of the HIPAA system supports communication and digital recording activities using the "AES-Encryption security control" in recent times. The convenience of the HIPAA system also encompasses digital connectivity and pre-registration applications for patient safety and better service management in healthcare. The affiliation of "Google Drive, Cloud IoT Core, Cloud SQL, and Cloud Storage" is aligned in the data storage and support in healthcare management. The convenience of digital communication and easy access to digital portals for patient care are relevant to HIPAA delivery support and software-driven solutions in recent times.

B. Impact of HIPAA-compliant Delivery System in Healthcare Security

The support of using the HIPAA-Delivery system is quite a convenient part when it has been used in the healthcare delivery system. The security and confidentiality of data exchange operations will result in one of the biggest convenient parts of data security [13]. Controlling the convenience of real-time tracking and data security of patient records are used within this segment. This is the convenient part of registering one of the biggest controls within the operational solutions within the healthcare practice. The implication of the HIPAA-compliant delivery system is convenient to use patient feedback and monitoring solutions within healthcare organizations. The core functions of the "AES Data Encryption system" broaden dynamic security and end-to-end communication within solutions.

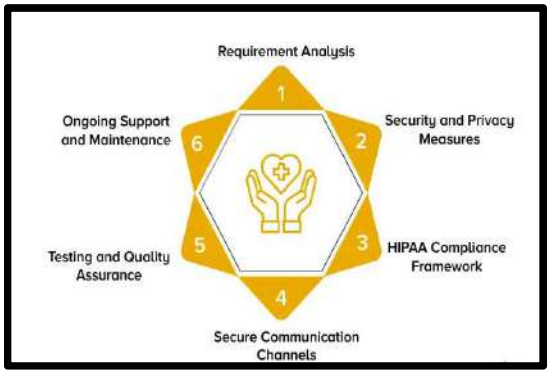

Figure 3: Impact of HIPAA Delivery System in Healthcare Operations

(Source: [3])

Quality assurance and mobility in communication channels are convenient to support the delivery and data tracking management. The orientation of the HIPAA delivery system helps to track the records of patients and providers of major services in patient care treatment. The complementary benefits of the HIPAA system allow mobility in data-driven analytics and support mobility in communication methods [17]. The digital connectivity and digital access activities allowed within the HIPAA delivery system increase mobility in the healthcare movement. The accessibility and SMART patient care supports are quite important to be enlisted within the HIPAA system in healthcare.

C. The Security and Efficient Healthcare Data Exchange

The importance of HIPAA-compliant delivery increases privacy and data security for patients in healthcare. In addition, digital pharmacy and treatment are quite convenient to be enlisted in security and healthcare management. The convenience of the "Streamline healthcare process" is also compressed in HIPAA controls and digital software support in this regard [18]. Predictive patient care and SMART recommendations in data security are responsible for the dynamic process of the HIPAA-compliant delivery system in recent times.

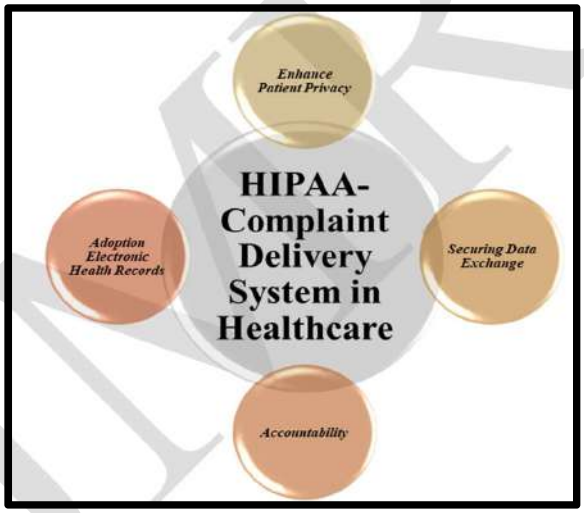

Figure 4: Benefits of HIPAA-compliant Delivery System in Healthcare Industry

(Source: Self-Created)

The accountability for patient care and protection from digital fraudulence are quite important to this segment. For example, "NextGen Healthcare, eClinicalWorks, Greenway Health, Athena Health, and Practice Fusion" are key healthcare organisations that are using HIPAA-compliant delivery practices [19]. The convenience of using the HIPAA system enabled mobilised communication and digital accessibility for patient care. The importance of using HIPAA security also encompasses a "Biometrics Security" in data security and social integrity. The convenience of Biometrics security is quite important to secure the solutions of operational communication and sustainability.

D. Recent Trends of HIPAA-compliant System

The trends in cyber security in healthcare HIPAA are the biggest support for effective patient care operations. Focusing on the contemporary HIPAA-compliant system, online portals for healthcare registration and patient data records have been enlisted in recent times. The contemporary usage of HIPAA-compliant delivery systems

helps to eliminate inconvenient communication and patient data tracking issues [20]. The medication and diagnostics information-sharing capabilities are also enlisted to the digital trends in the healthcare industry. The protection of PHI is another complementary part of registered within the trends of using HIPAA-compliant delivery systems.

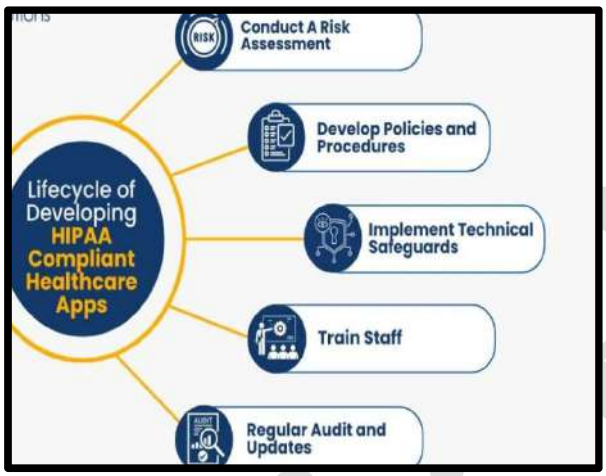

Figure 5: Trends of HIPAA-compliant Delivery System in Healthcare Industry

(Source: [5])

The trends in HIPAA-compliant delivery systems support regular auditing in data analytics while tracking patient records. The support in policies and regulatory risk assessment practice is further enlisted within the trends of HIPAA-compliant delivery systems within the healthcare industry.

III. METHODOLOGY

A. Research Design

The methodological construction of this study follows a research design to make a framework for data analytics. Focusing on the complementary design of this study a structure of "Explanatory Design" is a quality structure assisted within the research design. The usage of explanatory design is a convenient part of registering the explanatory research work and admittance of integrated data analytics for these data findings [21]. The effectiveness of explanatory design supports both "qualitative and quantitative methods" in research to allow a better transition of data synthesis. The usage of explaining centralised databases will help to identify the best solutions for data findings and support the methodological structure for this study.

B. Data Collection

Focusing on the next layer of this research a data collection process is a convenient part to mobilize the social support to the business configuration. The application of "qualitative and quantitative methods" combined within the data collection process to establish one of the best solutions for data analytics. A quantitative study focusing on the theoretical competencies and alliance to investigate HIPAA-compliant delivery systems in the healthcare industry has been followed. On the other hand, finding some secondary statistical referrals in data synthesis is the next part of methodological data collection using websites and scholars. Authentic sources such as "Google Scholar, PubMed, ProQuest, and JSTOR" are applied in the complementary solutions of data-driven analytics [18]. The possible solutions of data collection entitled The Best Findings regarding HIPAA-compliant Delivery System Analytics in the Healthcare System.

C. Case Studies/Examples

Case Study 1: Fortifying Home Wellness Screenings using HIPAA Safeguard Security Medtech Industry

The recent case scenario illustrates that fortification of home wellness in safeguarding tactics the usage of HIPAA is a convenient part of the healthcare system. The "American Heart Association (AHS)" supports the HIPAA digital monitoring and screening technologies for better patient care activities in healthcare development [5].

Case Study 2: HIPAA Compliance for Last-Mile Delivery Software in Medical Couriers of the Pharmaceutical Industry

The convenience of HIPAA-compliant software further assists in the "last-mile delivery process" in healthcare security. The controls in medical shipment are an operational part of registering the best solutions within HIPAA delivery security and it is further maintaining data security respectively [6].

Case Study 3: HIPAA-compliant VMS and App Development in US Government Hospitals

The installation and operational activities of HIPAA control the "VMS and app development" certifications within the healthcare industry. With the conjugation of healthcare security applications, it is quite convenient to enhance digital screening apps in healthcare to extend the "medical memory" for better patient care solutions [7].

D. Evaluation Metrics

The data evaluation metrics for Data exchange and security using "HIPAA-compliant delivery system" has found including effective challenges of cost convenience and technical faults. The disputes within errors and technical difficulties are relevant to tracking the data record for easy mobility within the healthcare controls. Apart from this, easy accessibility is another important metric to be enlisted within the evaluation of patient care convenience in HIPAA-compliant delivery systems.

IV. RESULTS

A. Data Presentation

The data interpretation about this research topic aligned with the current trends of HIPAA-Compliant Delivery systems used in the healthcare industry. The current trends of HIPAA security for patient care market reach have increased up to $226.3 million shares. On the other hand, the predicted values will be extended up to $325.72 million by the end of 2033-estimated prevalence of HIPAA in healthcare [20]. The usage of smart technologies within healthcare includes "IoT, AI, Automation, Augmented Reality, and Machine learning" to control the digital data record in the healthcare system.

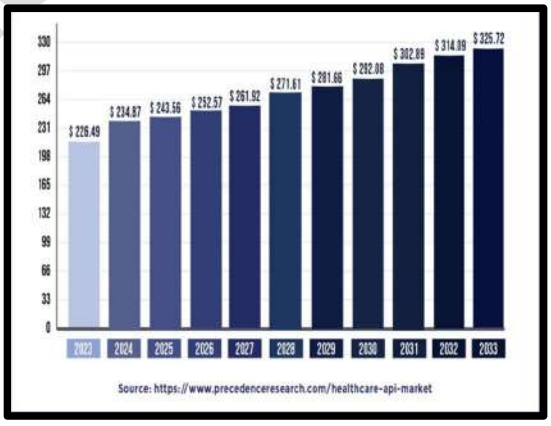

Figure 6: Healthcare Technology and SMART App Market Size

(Source: [8])

Illustration of data presentation the technological outputs are quite important to control HIPAA data security in healthcare. Encryption is the main element to be enlisted within the HIPAA-complaint delivery system to extend the beneficial outcomes of patient care.

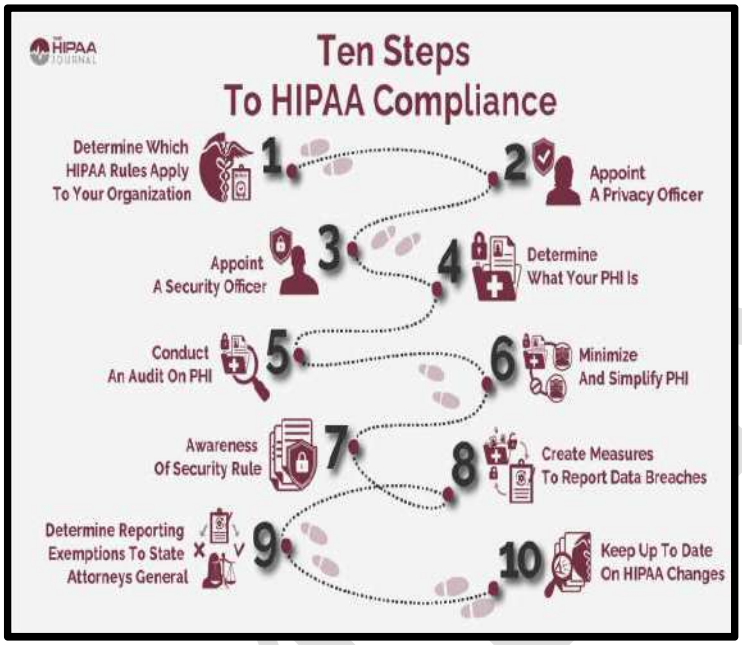

Figure 7: Technological Outcomes in HIPAA-Compliant System

(Source: [9]

Minimising the risks of PHI and taking screening over the data presentation is quite conventional to extend the balance of technological outcomes. The complementary HTTPS and SSL protocols indulged within the system are quite conventional to support the best outcomes from the security dynamics and enlist the best solutions within the business. The importance of AES encryption is an exquisite element to be enlisted within the data security and support of this business [22]. The essential outcomes of HIPAA security provide medical transcriptions and information sharing security for a better diagnosis. Easy tribal data and end-to-end information flow create a string of data security within the healthcare system in this regard.

B. Findings

Analysing the important findings from this research it has been encountered that data tracking and controlling operational data are convenient while using patient care management. The graphical representation of this presentation analyses the contemporary prevalence of HIPAA-compliant security control and its effectiveness in the healthcare industry. The significance of using HIPAA security protects patient support and provides beneficial convenience to records of accomplishment. Easy access and PHI risk control tracking are the convenient parts enlisted within the healthcare service mobilization [20]. Retrieving effective data backup and controlling data-centric designs to the HIPAA-compliant it has managed to develop the best supports to the operational convenience and enlisted the best support to the businesses respectively.

C. Case Study Outcomes

Case study	Company/Industry	Case study outcome	Relevance to current research
Fortifying Home Wellness Screenings	MedTech Industry	This study highlighted a glimpse of home care and wellness practices using HIPAA screening to enhance the medical care system in the MedTech industry of the UK [5].	The importance of this study is to highlight the monitoring practice and convenience of screening activities of HIPAA-compliant security for patient care.
Last-Mile Delivery Software in Medical Couriers	Pharmaceutical Industry	This study focuses on the last mile delivery system in pharmaceutical organizations such as "GSK, Pfizer, and AstraZeneca" which are using HIPAA for their healthcare treatment and customer support forum in recent times.	The relevance of this study is to highlight the convenience of HIPAA in last-mile delivery management to support data-tracking operations. Customer care-based support within last-mile delivery management is the most essential and convenient part to be enlisted within the evaluation of HIPAA in delivery management.
VMS and App Development	US Government Hospitals	The support of HIPAA in app development and VMS tools control are the main highlights of this study to enhance the healthcare service of US government-sponsored hospitals in recent times.	The relevance of this research highlights the beneficial usage of VMS and app development in healthcare convenience and data security values in US hospitals.

Table 1: Case Study Analysis

D. Comparative Analysis

Author	Focus	Findings	Gaps identified
[10]	This study focuses on AI-driven HIPAA-compliant cloud security in healthcare management.	The usage of artificial intelligence enabled a string of security and data-sharing channels for patient care resilience in the healthcare sector.	Lack of details within HIPAA-compliant configuration in technical solutions

[12]	The Laravel-based mHealth Apps is the main convenient part enlisted with the HIPAA technical compliance in medical care and security management in recent times.	The results of this article found that Laravel-based mHealth apps enabled pre-registration and enlisted data records to the patient to provide an easy and smart diagnosis for quick recovery.	The lack of complementary solutions to mHealth app disputes and contracts is addressed in this study.
[11]	This study highlights the contemporary challenges of HIPAA in software engineering and Medtech organizations.	The findings highlight that technical errors such as AI biases and complexes in encrypted databases are relevant to the scenario of potential issues highlighted within this scenario.	The poor interpretation of statistical analysis and quantitative review over the technical disputes in HIPAA technology for business.

Table 2: Comparison Analysis

V. DISCUSSION

A. Interpretation of Results

The results analyse both quantitative and qualitative research and present the achievable outcomes of each research objective. Analysing the contemporary usage of HIPAA-compliant delivery systems enabled major interactive and networking proficiency in the healthcare industry. The advantages of using HIPAA-compliant security control data records and tracking patient treatment records. Through convenience, the HIPAA-compliant service provides forecasting and diagnostic solutions to operational sustainability in healthcare [19]. Referral of organizations such as “NextGen Healthcare, eClinicalWorks, Greenway Health, Athena Health, and Practice Fusion” enabled this technology to establish the best healthcare outcome.

B. Practical Implications

The practical implications of using HIPAA-compliant technology are found assisting healthcare mobility in terms of communication and effective deliverables of performance mobility. The controls of data tracking and records are assisted by forecast analytics and predicting the future directions of patient care operations. The applications of HIPAA-Compliant are effective in determining the tendency and digital screening to establish home care settings in digital screening alignment. The resilience and sustainability in the technical form will be enhanced for the healthcare system using HIPAA-compliant solutions for business.

C. Challenges and Limitations

The potential limitations of this research are limited access to databases regarding HIPAA-compliant delivery systems within the potential solutions. The potential limitation of limited access to publicly available secondary databases is quite important to establish the main uncertainties within this study [17]. The potential issues of these limited resources will impact operational uncertainties and outcomes.

D. Recommendations

- ***Potential Usage of Expertise***
  1. The recruitment of technical expertise in the MedTech corporations for better operational mobility
  2. The utilization of expertise using greater resilience and controls over HIPAA-compliant activities for data tracking
- ***Training and Development within the Healthcare sector***

The implementation of training and development is quite convenient to allow better support within the technical facilities in the healthcare industry.

VI. CONCLUSION AND FUTURE WORK

The conclusive evidence of this research focuses on the HIPAA-compliant system for security and data exchange support in the healthcare industry. The AES encryption and PHI risk reduction are two essential areas covered regarding the beneficial advantage of HIPAA. On the other hand, technical disputes and controlling complexes are two major challenges identified within the operational activities of HIPAA. Future work might have a detailed value of current healthcare operations using HIPAA-compliant system solutions in data security.

VII REFERENCE LIST

1. Baumer, D., Earp, J. B., & Payton, F. C. (2009). Privacy of medical records: IT implications of HIPAA. *Computers & Security, 28*(1-2), 9-21.

2. Baird, A., & North, F. (2018). Personal health records: Design considerations for secure storage. *Journal of Medical Internet Research, 20*(3), e55.

3. Chintale, P., Korada, L., Ranjan, P., Malviya, R. K., & Perumal, A. P. (2021). The Impact of Covid-19 on Cloud Service Demand and Pricing in the Fintech Industry. Journal of Harbin Engineering University, 42(7).

4. Basile, G., & Zorkadis, V. (2020). Secure data exchange frameworks for healthcare using HIPAA-compliant cloud-based architectures. *Healthcare Informatics Journal, 26*(1), 45-67.

5. Cohen, I. G., Amarasingham, R., Shah, A., Xie, B., & Lo, B. (2018). The legal and ethical concerns of big data in health care. *Health Affairs, 37*(11), 1882-1889.

6. Dwork, C. (2006). Differential privacy. *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06)*, 1-12.

7. Feldman, S., Buchalter, S., & Hayes, L. (2018). Health data sharing and privacy regulations: What's needed for a HIPAA-compliant delivery system. *Journal of Health & Biomedical Law, 14*(2), 173-195.

8. Greene, A. H. (2012). Understanding the HIPAA Omnibus Rule: Compliance Strategies. *Journal of Health Care Compliance, 14*(5), 35-42.

9. Huesch, M. D., & Mosher, T. J. (2017). Using IT to improve compliance with HIPAA regulations. *Journal of the American Medical Informatics Association, 24*(3), 565-569.

10. Jang, S. (2016). Cybersecurity and HIPAA: Ensuring patient privacy in the digital age. *Healthcare Management Review, 41*(2), 138-147.

11. McGraw, D. (2013). Building public trust in uses of health insurance data: HIPAA and beyond. *Health Affairs, 32*(8), 1433-1441.

12. Mooney, G., & Pepper, G. (2019). Ensuring HIPAA compliance in a cloud-based world. *Journal of Business Ethics, 155*(3), 705-720.

13. O'Brien, T., & Yasnoff, W. A. (2020). Ensuring compliance with HIPAA for telemedicine data exchange. *Health Informatics Journal, 26*(1), 93-109.

14. Park, Y., & Lu, Q. (2021). Enhancing healthcare data security through blockchain and HIPAA compliance. *Journal of Cybersecurity and Privacy, 1*(1), 23-40.

15. Smith, H. J., & Milberg, S. J. (2019). Information privacy regulation: The evolving HIPAA framework. *MIS Quarterly, 43*(4), 981-1012.

16. Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in HIPAA-compliant systems. *Health Information Management Journal, 44*(3), 18-25.

17. Chintale, P. (2020). Designing a secure self-onboarding system for internet customers using Google cloud SaaS framework. IJAR, 6(5), 482-487.