

COMPARATIVE ANALYSIS OF CYBERSECURITY FRAMEWORKS FOR HEALTHCARE MOBILE APPS: ENSURING PRIVACY AND PROTECTION

Shara Mae R. Tee¹, Ramil Lumauag²

¹Central Philippines State University, ²Iloilo Science and Technology University
Corresponding author: tee.sharamae14@gmail.com, ramil.lumauag@isatu.edu.ph

Abstract

The rapid adoption of mobile applications in healthcare has revolutionized patient care, offering convenient access to medical services and sensitive health data. However, this advancement poses significant challenges in maintaining data privacy and security. This research provides a comparative analysis of prominent cybersecurity frameworks for healthcare mobile applications, including the Health Insurance Portability and Accountability Act (HIPAA), the ISO27001 and the National Institute of Standards and Technology (NIST) cybersecurity framework. Additionally, it explores the role of blockchain technology as an innovative solution to address emerging security challenges. The study evaluates these frameworks based on their core principles, adaptability to mobile platforms, and ability to mitigate risks such as unauthorized access, data breaches, and non-compliance with regulations. Blockchain technology, known for its decentralized architecture, immutability, and secure data sharing via smart contracts, is analyzed for its potential to enhance the security of healthcare applications. This research highlights the synergy between established frameworks and blockchain technology, illustrating how their integration can create a robust security infrastructure for healthcare mobile apps. The findings emphasize the need for a comprehensive strategy that combines regulatory compliance with advanced technologies to safeguard sensitive healthcare information, ensure user trust, and promote resilience in digital healthcare systems. The insights from this study aim to guide developers, healthcare providers, and policymakers in adopting innovative cybersecurity measures, addressing the unique challenges of the healthcare sector in an increasingly mobile-driven world.

Keywords: Cybersecurity framework, Healthcare mobile applications privacy and protection.

INTRODUCTION

As the reliance on mobile applications in healthcare continues to grow, understanding the intricate relationship between technology and regulatory measures becomes increasingly critical for safeguarding sensitive patient information. Patients data is not only a vital asset for healthcare providers but also a target for cyber threats, making it essential to implement robust security measures that align with both technological advancements and legal requirements. (Alvarenga & Tanev, 2017) According to recent studies, a significant percentage of healthcare organizations have reported experiencing data breaches, highlighting the urgent need for comprehensive cybersecurity protocols that can adapt to evolving threats and ensure patient trust in digital health solutions. (Alsaghier and Ahamad)

Establishing a proactive approach to cybersecurity, including regular assessments and employee training, can help mitigate risks and foster a culture of security awareness within healthcare organizations. (Quasim *et al.*, 2020) By enhancing security measures and investing in advanced technologies such as encryption and intrusion detection systems, healthcare providers can better protect sensitive patient information from unauthorized access and potential exploitation. The security of mobile applications in healthcare is a pressing concern, as evidenced by various studies highlighting vulnerabilities that could compromise patient data. One of the key strategies to

address these vulnerabilities involves implementing rigorous testing and validation processes during the development of mobile health applications, ensuring that security features are integrated from the outset rather than as an afterthought. (Chakraborty *et al.*, 2019)

These vulnerabilities can be mitigated and safeguarded by an effective cybersecurity framework that includes regular updates, employee training, and incident response plans to swiftly address any breaches that may occur. (Iqbal & Matulevičius, 2021) The cybersecurity frameworks for healthcare mobile applications, such as Health Insurance Portability and Accountability Act (HIPAA), the ISO27001, and the National Institute of Standards and Technology (NIST) cybersecurity framework and blockchain technologies, serve as essential guidelines for protecting sensitive patient data and maintaining compliance with legal requirements. By leveraging these frameworks, developers can create more robust applications that not only protect user information but also enhance trust among users in the healthcare system. (Alvarenga and Tanev)

However, the rapid evolution of cyber threats necessitates continuous adaptation and improvement of these frameworks to stay ahead of potential vulnerabilities. According to one study, nearly 80% of healthcare organizations reported experiencing a data breach in the past two years, highlighting the urgent need for enhanced security measures and proactive risk management strategies. (Coventry & Branley, 2018) As the healthcare industry increasingly adopts digital solutions, identifying the need for balanced cybersecurity strategies is crucial to ensure that patient data remains secure while still allowing for innovation and efficiency.

LITERATURE REVIEW

A. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards for the protection of sensitive patient information, mandating that healthcare organizations implement safeguards to ensure confidentiality and integrity. (Zhu *et al.*) Compliance with HIPAA not only helps protect patient information but also fosters trust between patients and healthcare providers, which is essential in maintaining a robust healthcare system. This cybersecurity strategy must encompass not only technical measures but also employee training and awareness programs, as human error remains a significant vulnerability in safeguarding sensitive data. (Arain *et al.*)

The principles of HIPAA emphasize the importance of a comprehensive approach to data protection, which includes regular audits and assessments to identify potential weaknesses in security protocols. The HIPAA Framework consists of several key components designed to guide healthcare organizations in their efforts to secure patient information effectively, including administrative safeguards, physical safeguards, and technical safeguards that collectively work to mitigate risks associated with data breaches (Thamilarasu & Lakin).

The Health Insurance Portability and Accountability Act (HIPAA) plays a crucial role in ensuring the privacy and security of personal health information (PHI) within health care mobile applications, commonly known as mHealth apps. These apps, which allow users to manage and access their health data, must comply with HIPAA regulations to protect sensitive information. However, many developers lack awareness of these guidelines, leading to potential risks of data breaches. This necessitates the development of tools and frameworks to aid in maintaining HIPAA compliance during app development and usage. According to (Saha *et al.*, 2023), HIPAA compliance ensures that PHI is securely transmitted, received, and stored, safeguarding users' privacy and trust in digital

health solutions. mHealth apps are increasingly used for managing health records, necessitating strict adherence to HIPAA to protect PHI from unauthorized access and breaches.

1. Security Algorithm

The security regulations establish protocols that protect the integrity, confidentiality, and availability of health data. Specifications exist to delineate various perspectives that govern administrative, physical, technical, and communication provisions. To safeguard and regulate patient health information, an effective security mechanism must be established to shield electronic forms of PHI from potential threats, including compromised security and unauthorized access. (Almuhammadi & Alsaleh, 2017)

2. Confidentiality

Encryption is the most effective and prevalent method for ensuring health data confidentiality in accordance with security regulations. It can render the PHI unreadable during storage and electronic transmission. Therefore, encryption is an effective method for safeguarding electronic PHI and preventing unauthorized disclosure.

3. Data Integrity

Compliance with security regulations necessitates the protection of the integrity of electronic health information. A patient's life may be jeopardized if a physician prescribes an unsuitable medication due to alterations in their drug allergy history. The alteration or deletion of medical data and unauthorized destruction of health information is impermissible. Consequently, to ensure patient safety, data integrity must be assured.

B. ISO27001

The International Organization for Standardization (ISO) is a non-governmental organization headquartered in Geneva has issued over 22,600 standards applicable across various industries. It includes a broad variety of procedures associated with the administration of IT risk and the safeguarding of data. (Alshar'e, 2023) The framework for developing an information systems management system is delineated. The ISO 27001 standards are widely recognized as a reliable foundation for security management. Assessment is conducted on the requirements for establishing, executing, and enhancing information security management systems. Enhancing the security of a company's sensitive data can be achieved through various methods, one of which involves the adoption of ISO standards.

The implementation of ISO ensures data reliability, consistent availability, and ongoing security maintenance. An audit of an ISO framework is performed in two phases. The initial phase of the audit is termed the "documents review," during which the auditor examines the written records of the system's operations, policies, and procedures to assess compliance with ISO 27001. An on-site review constitutes the second step, referred to as the "certification audit." The objective of this phase is to ascertain whether the organization has established an ISMS in accordance with ISO 27002. ISO certification is valid for a period of three years, after which it requires renewal. (Ananda Muhamad Tri Utama, 2022)

C. National Institute of Standards and Technology (NIST) cybersecurity framework

NIST would function as an autonomous agency that collaborates closely to develop and implement standards, measurements, and technologies for commerce. It was established in 1901. The National Institute of Standards and Technology (NIST) has established a cybersecurity framework to aid enterprises in addressing cybersecurity issues. This approach emphasizes

business drivers to aid organizations in guiding their cybersecurity initiatives and integrating cybersecurity risks into risk management processes. The Cybersecurity Enhancing Act of 2014 amended the original version established under Executive Order 13,636. The framework offers risk principles and best practices applicable to both small and large enterprises, irrespective of their focus, sector, or geographical location. (National Institute of Standards And Technology, 2018)

- Core processes: are identification, protection, detection, reaction, and recovery. To mitigate concerns regarding cybersecurity, the framework employed these components. These actions, divided into 23 activities, encompassed all aspects of establishing a cybersecurity program and the essential components of risk management systems.
- Levels of implementation: The NIST CSF utilized a scoring system with points from 0 to 4 to establish an overall score that the organization could use as a benchmark for its risk maturity level.
- Profiles: It is advantageous for organizations to assess their existing risk tolerance level. Moreover, it instructs the organization on mitigating risks and elevates the importance of security measures, both of which are advantageous results. By comparing its current profiles to its ideal profiles, the company may more efficiently allocate its resources to enhance its security management over time, thereby facilitating expansion.

Nist Cybersecurity Framework

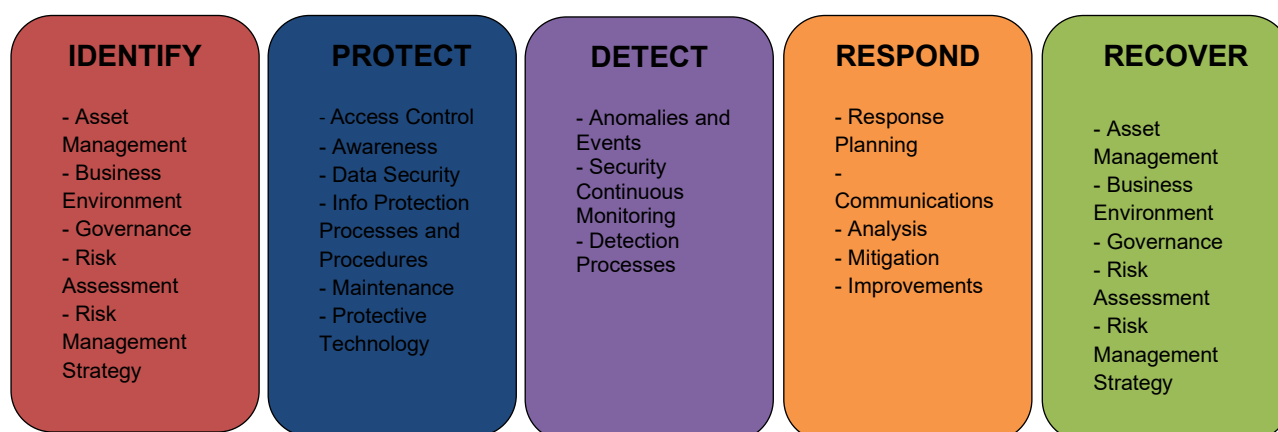


Figure 1. NIST Cybersecurity framework (Khaleefah & Al-Mashhadi, 2024)

The system model comprises five simultaneous and continuous operations (recognize, guard, detect, respond, and restore), classifications and definitions of subclasses for each activity, and instructional references for every subclass provided by the core, implementation tiers, and profile of an existing framework. The Framework Core comprises concurrent and continuously operating functions, including Identify, Protect, Discover, Respond, and Recover, along with classes and subclasses that delineate anticipated outcomes for each function.

D. Blockchain Technology

Blockchain technology operates through cryptographic techniques to generate interconnected information blocks, each containing essential data to authenticate its legitimacy and facilitate the creation of subsequent blocks.(Monrat *et al.*, 2019) Furthermore, blockchain functions as a distributed database, which enables it to achieve significant attributes such as privacy protection,

immutability, and decentralization, thereby facilitating secure data sharing. (Ali Syed *et al.*, 2019) The extensive advancement of blockchain technology is prevalent in the energy sector, vehicular networking, and healthcare. (Chen *et al.*, 2021) Nonetheless, the extensive implementation of blockchain technology and the ongoing advancement of new technologies are perpetually intensifying the challenges and threats associated with blockchain technology. The integration of blockchain technology in the healthcare sector may involve all facets of hospital systems, including processes, oversight, data management, finance, auditing, and record-keeping, while also offering essential technical support for restructuring hospital informatization and workflows. (Hussien *et al.*, 2021)

From a technical standpoint, blockchain is not an innovative technology but rather a compilation of pre-existing technologies.

- The peer-to-peer network employs an immutable distributed ledger, guaranteeing the structural immutability of the single node ledger via the blockchain data structure.
- Security technologies, including encryption, cryptography, and hash algorithms, ensure the security and privacy of transactions.
- Consensus algorithms: a mathematical framework for collective verification of blockchain, designed to establish trust among all parties and utilize technology to guarantee the integrity of consensus outcomes.
- Smart contract: In 1994, Nick Szabo introduced the concept of the smart contract, characterized by a collection of agreements that enable participants to enforce their commitments. Smart contracts ensure reliable business transactions without the need for intermediaries, primarily aiming to enhance security and minimize transaction costs associated with other contracts. Consequently, smart contracts guarantee that all transactions among the nodes are trustworthy and dependable. (Kairaldeem *et al.*, 2021)

Additionally, Blockchain is fundamentally a distributed ledger technology that creates a decentralized, machine-trusted, and collectively shared ledger system, employing an optimal mathematical solution to establish trust and consensus among all participants.

- Transparency and accessibility: the system is available to all participants, who possess the right to access and equally benefit from blockchain information. The consensus is achieved by the voting of specific nodes to expedite verification and confirm transactions in a reduced timeframe. If multiple nodes can achieve consensus without the associated interests in a transaction, it reflects the network's consensus.
- Equitable competition: the functions of all nodes are computed by algorithms, which also dictate the rights to accounting.
- Authenticity and integrity: every record is documented accurately and comprehensively under supervision.
- Secure and dependable: data encryption and cryptographic techniques thwart tampering and forgery; the intricate checksum sharing mechanism guarantees integrity, availability, and confidentiality. Multiple assailants are identified via an encryption standard (digital signature) wherein each node possesses its own key, and packet transmission occurs only when the key is in a valid condition. (Talukdar *et al.*, 2021)

Health information is gathered from diverse medical data sources and intricate data forms. Data sharing facilitates EHR interaction among various healthcare platforms; however, it jeopardizes patient privacy. Blockchain technology faces numerous technical challenges that hinder its extensive adoption in the healthcare sector. (Hussien *et al.*, 2021)

- Constrained transaction performance and scalability: the blockchain's restricted transaction processing capability and the protracted duration for transactions to be aggregated into blocks.
- Inadequate privacy safeguards: while blockchain is tamper-proof and decentralized, the transparency of the user's ledger to participating organizations allows any organization to access the same data. The exposure of users' private data on the blockchain will exacerbate the risk of privacy breaches. In contemporary public blockchain systems like Bitcoin, all transaction details, including amounts, are accessible to the public. This indicates non-compliance with certain regulatory privacy standards, including the General Data Protection Regulation (GDPR). (Hussien *et al.*, 2021)

Below is the six-layer system architecture of blockchain technology. Each layer can be divided into two components: the fundamental module and the security module. The basic module serves as the fundamental component for executing the primary functions of this layer, while the security module functions as a protective component to guarantee the security of each layer and deliver reliable technical support for the upper layer.

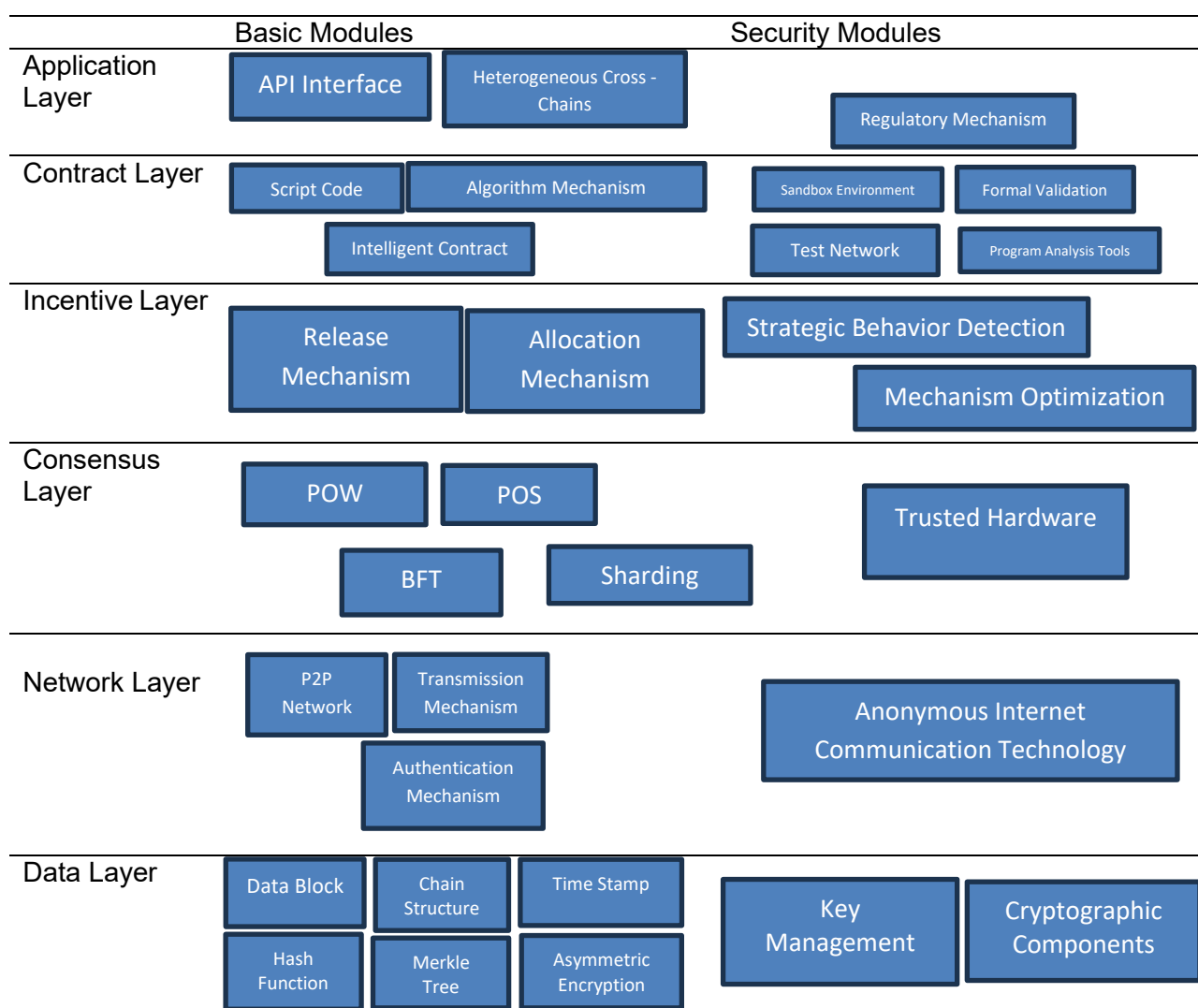


Figure 2. The blockchain system architecture

The security model incorporated within the data layer, along with other cryptographic elements, serves as the foundation for the implementation of the remaining five-layer functions. The network layer encompasses various network technologies, with its primary function being to facilitate the legitimate connection and efficient communication among blockchain nodes. The consensus layer ensures that the node maintains a uniform valid perspective and communication protocol as dictated by the blockchain network, dedicated to developing a more secure, efficient, and low-energy consensus mechanism. The incentive and consensus layers are mutually dependent to ensure the security and stability of the blockchain system collectively. The design of the consensus mechanism will influence the choice of incentive entities and the strategy for incentive distribution; likewise, the design of the incentive mechanism is interconnected with the security of the consensus mechanism and the stability of the blockchain. A smart contract is a computer program that executes automatically based on predetermined contractual terms between the buyer and seller, encompassing the code and data required for deployment, which constitutes the core of the contract layer. The application layer must represent business functions across various scenarios, and the architectural design will exhibit minor variations. The application layer directly engages with users and must exhibit a degree of uniformity in architectural design.

Blockchain technology represents a recent advancement in information technology, enabling network participants to record transactions and immediately disseminate them to other blockchain users.(Attaran, 2022) Blockchain was employed in various research studies to address the deficiencies of existing Electronic Health Records (EHR) systems.(Esposito *et al.*, 2018) Furthermore, by storing the hash of cloud data on the blockchain, they addressed security and privacy issues related to medical records.(Meri *et al.*, 2017)Nonetheless, the systems are vulnerable to a single point of failure in these operations due to the cloud server. Moreover, the technique fails to address the concern of patient privacy when medical records are stored in a centralized cloud database. Numerous research studies, (Griggs *et al.*, 2018) (XIA *et al.*, 2017) (Fan *et al.*, 2018)advocate for the utilization of blockchain technology to store medical data in a distributed ledger, thereby addressing the problem of a single point of failure.

Comparative Analysis

Table 1. Comparative Analysis for the advantages, limitations, threat mitigation and mobile adaptability

Framework	Advantages	Limitations	Threat Mitigation	Mobile Adaptability
ISO27001	• Uses Security Policies • Follows Asset Management • Emphasizes Asset Management • Emphasizes on human resources security • Focuses on communication and management of operations	• High Implementation Costs • Complexity in Implementation • Time-Consuming Certification Process • Frequent Updates and Maintenance • Potential Misalignment with Organizational Needs	• Risk Assessment and Management • Incident Response and Recovery • Continuous Monitoring • Physical and Environmental Security	• Support for Mobile Device Security • Remote Access Policies • Encryption for Data Transmission

NIST Cybersecurity Framework	• Focuses on business continuity. • Has policies and procedures adhered to • Uses standard operation procedures • Emphasizes on personal security • Involves awareness and trainings • Risk Mitigation	• Resource-Intensive Implementation • No Certification Mechanism • Focus on High-Level Strategies • Ongoing Maintenance Challenges • Potential Misalignment with International Standards	• Holistic Risk Management • Core Functions for Threat Response • Detailed Subclasses for Threat Handling • Continuous Monitoring and Adaptation • Incident Response Framework	• Encryption for Mobile Data • Real-Time Threat Detection • Incident Response for Mobile Platforms • Global and Flexible Application
Blockchain Technology	• Reduce cost and increase efficiency • Secure, accessible, and real-time. • Network transactions database. • Better security against “pushing”. • Easy communication in the more extensive network.	• Cost-effectiveness has yet to be proven. • Insecure with data leaking issue. • Regulatory issues and technical challenges. • Risk for potential compromise of data set. • Smaller networks pose the same concern.	• Data Security and Privacy • Tamper Resistance • Consensus Mechanism • Protection Against Single Points of Failure	• Efficient Data Sharing • Scalability Challenges • Enhanced Transparency

As summarized in Table 1, ISO 27001, NIST Cybersecurity Framework (CSF), and blockchain technology are all unique approaches to managing information security, contributing to the protection of organizational data. ISO 27001 is a globally recognized and reliable foundation for information security management systems, emphasizing continuous monitoring and improvement of security practices. However, its implementation can be resource-intensive, especially for small to medium-sized organizations. NIST CSF is a comprehensive framework designed to guide organizations in improving their cybersecurity practices through its five core functions: Identify, Protect, Detect, Respond, and Recover. It integrates cybersecurity risks into broader organizational risk management processes, offering a flexible and adaptable approach for organizations of all sizes and sectors. Blockchain technology operates through cryptographic techniques to create interconnected data blocks, ensuring authenticity, privacy, and immutability. It enhances secure data sharing across

various sectors, such as healthcare, energy, and vehicular networking. However, it faces challenges such as constrained transaction performance, scalability, and privacy risks associated with transparency.

RESULTS AND DISCUSSION

ISO 27001, NIST CSF, and blockchain technology are all closely linked to HIPAA, which sets national standards for protecting sensitive patient information in healthcare systems. HIPAA regulations require organizations to implement robust safeguards to ensure the confidentiality, integrity, and availability of PHI. These frameworks, which emphasize continuous risk assessments, vulnerability identification, and clear security protocols, can help organizations maintain HIPAA compliance. ISO 27001 provides a systematic approach to establishing an Information Security Management System (ISMS) that supports HIPAA's administrative safeguards. NIST CSF, with its core functions, can guide organizations in implementing technical and administrative measures to mitigate risks and enhance data security.

Blockchain technology, with its decentralization, cryptographic security, and immutability, offers a potential solution to safeguard PHI, particularly in mHealth apps. It can enhance data protection by ensuring secure, tamper-proof transaction records and potentially mitigate risks related to unauthorized access. HIPAA compliance for mobile health applications is crucial, as they often store and transmit patient data. Integrating ISO 27001, NIST CSF, and blockchain technology into mHealth app development can help safeguard against potential data breaches, protect patient privacy, and maintain trust in digital health solutions.

CONCLUSION

In conclusion, the integration of **ISO 27001**, **NIST CSF**, and **blockchain technology** not only strengthens an organization's approach to managing cybersecurity risks but also provides a reliable means of achieving HIPAA compliance. Together, these frameworks and technologies ensure that healthcare providers can protect patient information effectively, safeguard against cyber threats, and foster trust between healthcare organizations and patients. This comprehensive approach is especially important as the healthcare sector increasingly relies on digital and mobile solutions for managing patient data.

REFERENCES

- Ali Syed, T., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access*, 7, 176838–176869. <https://doi.org/10.1109/ACCESS.2019.2957660>.
- Almuhammadi, S., & Alsaleh, M. (2017). *Information Security Maturity Model for Nist Cyber Security Framework*. 51–62. <https://doi.org/10.5121/csit.2017.70305>.
- Alsaghier, Hisham M., and Shaik Shakeel Ahamad. "A Secure Robust and Privacy Enhance Mobile Healthcare Framework." *International Journal of Web Services Research*, July 2018, doi:10.4018/IJWSR.2018070104.
- Alshar'e, M. (2023). Cyber Security Framework Selection: Comparision of Nist and Iso27001. *Applied Computing Journal*, 3(1), 245–255. <https://doi.org/10.52098/acj.202364>.

- Alvarenga, A., & Tanev, G. (2017). A Cybersecurity Risk Assessment Framework that Integrates Value-Sensitive Design. *Technology Innovation Management Review*, 7(4), 32–43. <https://doi.org/10.22215/timreview/1069>.
- Ananda Muhamad Tri Utama. (2022). No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title. 9(July), 356–363.
- Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, 15(1), 70–83. <https://doi.org/10.1080/20479700.2020.1843887>.
- B. Krumay, E. W. N. Bernroider and R. Walser, "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework," *Secure IT Systems*, vol. 11252, pp. 369–384, 2018.
- Chakraborty, S., Aich, S., & Kim, H. C. (2019). A Secure Healthcare System Design Framework using Blockchain Technology. *International Conference on Advanced Communication Technology, ICACT*, 2019-February(May), 260–264. <https://doi.org/10.23919/ICACT.2019.8701983>.
- Chen, J., Wang, W., Zhou, Y., Ahmed, S. H., & Wei, W. (2021). Exploiting 5G and Blockchain for Medical Applications of Drones. *IEEE Network*, 35(1), 30–36. <https://doi.org/10.1109/MNET.011.2000144>.
- 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>.
- Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, 5(1), 31–37. <https://doi.org/10.1109/MCC.2018.011791712>.
- Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, 42(8), 1–11. <https://doi.org/10.1007/s10916-018-0993-7>.
- Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, 42(7), 1–7. <https://doi.org/10.1007/s10916-018-0982-x>.
- Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., & Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, 22(March), 100217. <https://doi.org/10.1016/j.jii.2021.100217>.
- Iqbal, M., & Matulevičius, R. (2021). Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications. *Lecture Notes in Business Information Processing*, 428(August), 67–84. https://doi.org/10.1007/978-3-030-85867-4_6.
- Kairaldeem, A. R., Abdullah, N. F., Abu-Samah, A., & Nordin, R. (2021). Data Integrity Time Optimization of a Blockchain IoT Smart Home Network Using Different Consensus and Hash Algorithms. *Wireless Communications and Mobile Computing*, 2021(MI). <https://doi.org/10.1155/2021/4401809>.
- Khaleefah, A. D., & Al-Mashhadi, H. M. (2024). Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review. *Iraqi Journal of Science*, 65(1), 468–486. <https://doi.org/10.24996/ijis.2024.65.1.38>.
- Meri, A., Hasan, M. K., & Mohd Satar, N. S. (2017). The Healthcare Professionals to Utilize Cloud Computing Services. *Asia-Pacific Journal of Information Technology & Multimedia*, 06(02),

31–42. <https://doi.org/10.17576/apjitm-2017-0602-04>.

- Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7, 117134–117151. <https://doi.org/10.1109/ACCESS.2019.2936094>.
- National Institute of Standards And Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity 重要インフラのサイバーセキュリティを改善するためのフレームワーク*. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf%0Ahttps://doi.org/10.6028/NIST.CSWP.04162018>.
- Quasim, M. T., Algarni, F., Radwan, A. A. E., & Alshmrani, G. M. M. (2020). A Blockchain based Secured Healthcare Framework. *2020 International Conference on Computational Performance Evaluation, ComPE 2020*, 386–391. <https://doi.org/10.1109/ComPE49325.2020.9200024>.
- R. Kissel, "Glossary of Key Information Security Terms," NISTIR 7298, 2019.
- Talukdar, M. I., Hassan, R., Hossen, M. S., Ahmad, K., Qamar, F., & Ahmed, A. S. (2021). Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature. *Wireless Communications and Mobile Computing*, 2021. <https://doi.org/10.1155/2021/6693316>.
- XIA, Q., SIFAH, E. B., KWAME OMONO ASAMOAH, J. G., DU, X., & GUIZANI, M. (2017). MedDShare : Trust-less Medical Data Sharing Among. *IEEE Access*, 5, 1–10.
- Zhu, Shanying, *et al.* "Achieving Data Security and Privacy across Healthcare Applications Using Cyber Security Mechanisms." *The Electronic Library*, Dec. 2020, doi:10.1108/EL-07-2020-0219.