„Krytyka Prawa", tom 17, nr 4/2025, s. 117–132, ISSN 2080-1084, e-ISSN 2450-7938, © 2025 Authors.

RANEETA PAL[1], SONY KULSHRESTHA[2], RAVI KANT[3]

Use of Emerging Technologies to Address Legal and Cyber Governance Issues of Protected Health Information (PHI)[4]

Submitted: 30.01.2025. Accepted: 24.06.2025

Abstract

The healthcare sector cannot work in isolation. For healthcare professionals to perform their duties effectively, it is necessary to know, collect, and analyse the most intimate details of a patient's health. Health data have extraordinary potential and require protection from accidental or intentional cyberattacks. It is therefore imperative that healthcare providers maintain the confidentiality of patients' health-related information. This article examines the use of emerging technologies in addressing the legal and cyber governance issues surrounding Protected Health Information (PHI). Special attention is given to emerging technologies such as blockchain, artificial intelligence, machine learning, and homomorphic encryption as effective tools for safeguarding health data. The paper also considers regulatory compliance and standards, providing deeper insights into the best practices adopted in different countries. It concludes by outlining key challenges and offering suitable recommendations to address them.

Keywords: emerging technologies, protected health information, cyber governance, data privacy, regulatory framework.

1 Raneeta Pal – Research Scholar, Department of Law, Manipal University Jaipur (India), e-mail: palraneeta@gmail.com; ORCID: 0000-0002-8514-880X.

2 Dr. Sony Kulshrestha – Associate Professor, Faculty of Law, Manipal University Jaipur (India), e-mail: sony.kulshrestha@jaipur.manipal.edu; ORCID: 0000-0002-8184-4998.

3 Ravi Kant, PhD – Assistant Professor Symbiosis Law School, Pune Symbiosis International (Deemed University), Pune (India), e-mail: ravikant.9.rk@gmail.com; ORCID: 0009-0004-6630-0951.

4 The research in this article has not been supported financially by any institution.

 DOI: 10.7206/kp.2080-1084.817

„Krytyka Prawa", tom 17, nr 14/2025, s. 117–132, ISSN 2080-1084, e-ISSN 2450-7938, © 2025 Authors.

RANEETA PAL, SONY KULSHRESTHA, RAVI KANT

Wykorzystanie nowych technologii w kontekście kwestii prawnych i zagadnień cyberzarządzania dotyczących chronionych informacji zdrowotnych (PHI)[5]

Streszczenie

Sektor ochrony zdrowia nie może funkcjonować w izolacji. Aby specjaliści medyczni mogli skutecznie wykonywać swoje obowiązki, konieczne jest poznanie, gromadzenie i analizowanie najbardziej intymnych informacji dotyczących zdrowia pacjentów. Dane zdrowotne mają ogromny potencjał i wymagają ochrony przed przypadkowymi lub celowymi cyberatakami. Dlatego tak istotne jest, aby podmioty lecznicze zapewniały poufność informacji związanych ze stanem zdrowia pacjentów. Niniejszy artykuł analizuje wykorzystanie nowych technologii w rozwiązywaniu problemów prawnych oraz zagadnień z zakresu cyberzarządzania dotyczących chronionych informacji zdrowotnych (PHI). Szczególną uwagę poświęcono technologiom takim jak blockchain, sztuczna inteligencja, uczenie maszynowe oraz szyfrowanie homomorficzne, które stanowią skuteczne narzędzia ochrony danych zdrowotnych. W artykule omówiono również kwestie zgodności regulacyjnej i obowiązujących standardów, dostarczając pogłębionych informacji na temat najlepszych praktyk stosowanych w różnych krajach. Tekst kończy się przedstawieniem kluczowych wyzwań oraz odpowiednich rekomendacji mających na celu ich rozwiązanie.

Słowa kluczowe: nowe technologie, chronione informacje zdrowotne, cyberzarządzanie, prywatność danych, ramy regulacyjne.

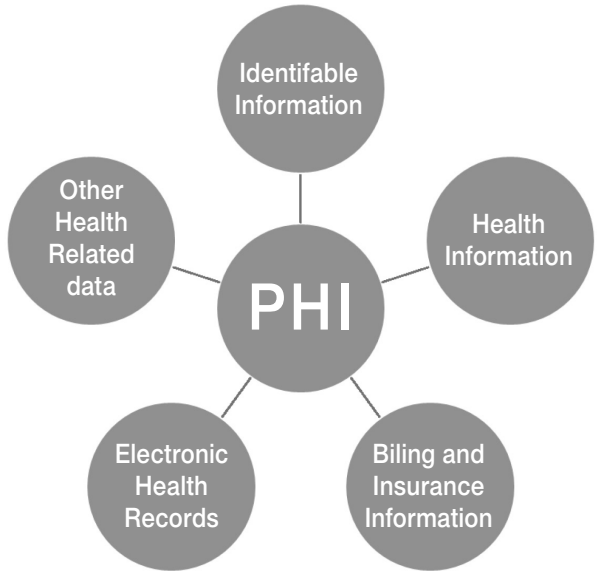
[5] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

Introduction

Protected Health Information (PHI) refers to demographic identifiers, dates on which healthcare services were provided, financial details of the patient, and notes about the individual's medical treatment or history made by a healthcare provider. PHI encompasses information that healthcare institutions may collect regarding the healthcare status of a particular individual, which includes their physical or mental health history, condition or treatment, operations and products used for the same, and all other facts that relate to a particular individual. This includes a host of data forms, including the patient's health records, diagnostic test results, proposed and prescribed medications or dosages, insurance-related data, and even fingerprints or genetic data. The records stored on paper are referred to as paper-based records, whereas those stored in electronic format fall under Electronic Health Records (EHRs).

PHI is created and shared within different settings in the healthcare system, which includes hospitals, clinical facilities, pharmacies, insurance providers, mobile health applications, and wearable devices.

Figure 1. Types of PHI



 DOI: 10.7206/kp.2080-1084.817

Protected Health Information (PHI) is defined as any data that relate to an individual's health, illness, or treatment, which render the person identifiable. This information is stored and used by insurance companies, healthcare professionals, and various health technology-related devices and applications. Some of the information included in PHI comprises the patient's health records, test results such as x-rays, laboratory data, and results of other tests, prescribing details of medicine, bills and accounts, genetic data, and many others. PHI is broad in scope; any data that can be associated with an individual may be included. This extends to demographic data such as names, addresses and dates of birth, along with identifiers such as Aadhaar numbers where they are linked to health information.

The specificity and comprehensiveness of PHI are often defined and regulated by certain legal acts – such as HIPAA in the USA and GDPR in the EU. The objective of these laws is to establish specific guidelines on how PHI can be collected, shared, stored, and accessed to ensure the privacy and security of the relevant data.

This study seeks to address the following research questions: How can emerging technologies effectively address legal and cyber governance challenges related to PHI? What are the comparative strengths and limitations of technologies such as blockchain, AI, and homomorphic encryption in protecting PHI? What best practices and regulatory frameworks can support the safe adoption of these technologies in healthcare?

Methodology

This study adopts a doctrinal and qualitative research approach to investigate the governance of Protected Health Information (PHI) within the healthcare sector, focusing on its legal, ethical, and operational dimensions. As part of this project, thorough review of relevant literature, case studies, and legal frameworks governing the protection of PHI has been conducted. The analysis uses thematic techniques to uncover emerging patterns and trends, while also comparing different regulatory models to evaluate their efficacy. Data were collected from both primary and secondary sources. The primary sources include legislation governing data privacy in the digital healthcare sector of India, the USA, and the UK. The secondary sources include articles, books, journals, commentaries, and conference proceedings.

Emerging Technologies for Protecting PHI

Technology	Key Features	Applications in PHI Protection
Blockchain Technology	Decentralised, Immutable, Transparent	Patient-centric control, Interoperability, Auditability
Artificial Intelligence (AI)	Anomaly Detection, Predictive analytics	Automated Compliance, Enhanced data-level encryption, Robust access control
Homomorphic Encryption	Secure computations on encrypted data	Privacy-preserving data sharing, Secure data processing, Regulatory compliance

Blockchain Technology

Blockchain technology is emerging as a revolutionary solution for enhancing the protection of PHI. Blockchain is a decentralised ledger that secures data through a method that is not only transparent but also immutable, recording transactions across a network of computers. The aspects of blockchain that make it decentralised also make it an appropriate solution to many PHI security dilemmas.

1. **Decentralisation and Security**: Traditional databases store PHI in centralised systems, which are vulnerable to single points of failure, making them prime targets for cyberattacks. Blockchain distributes data across a network of nodes, eliminating these central points of vulnerability. Each node holds a copy of the entire blockchain, making it highly resistant to breaches and tampering.
2. **Immutability and Auditability**: Blockchain technology serves as an immutable record-keeping system in which data once recorded cannot be erased or altered. This guarantees the security of PHI, since any attempt to alter a record is immediately reflected throughout the network.[6] The use of blockchain enhances auditability, as every transaction is logged to create a clear and transparent record of who accesses patients' PHI and any changes made to it.
3. **Smart Contracts and Access Control**: Smart contracts are self-executing pieces of code embedded within the blockchain infrastructure that automatically activate when predetermined conditions are met. They can automatically enforce access control and permissions, which means that no third

[6] S. Lincke, *Planning for Network Security*, [in:] *Information Security Planning*, Springer, Cham 2024, p. 147.

 DOI: 10.7206/kp.2080-1084.817

party without authorised rights can access or modify a patient's health data. For example, one application could grant a physician access once a patient provides electronic consent through a digital signature.

4. **Patient-Centric Control**: Blockchain-based solutions can return meaningful control of personal information to patients. By sharing consent and key-management responsibilities with patients, blockchain systems allow them to define access rights and monitor the usage of their PHI. This patient-empowering approach strengthens privacy and trust.
5. **Interoperability**: Blockchain can enhance interoperability across diverse healthcare systems by enabling data sharing on a single platform. This helps minimise instances where PHI is inconsistent or outdated among multiple providers, thereby improving the coordination of treatment while ensuring robust protection of patient information.
6. **Challenges and Limitations**: Despite its promise, blockchain faces challenges related to scalability and high computational resource requirements, which can hinder widespread adoption in large healthcare systems. Moreover, integrating blockchain with existing legacy systems can be complex and costly. There are also concerns around data immutability, as erroneous entries cannot be easily corrected once recorded and stored.

Artificial Intelligence (AI) and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are among the most novel technologies that have been developed to enhance the protection and privacy of Protected Health Information (PHI). These technologies have therefore become vital in present-day practice, as they provide effective means of handling complex health information and preserving identified sensitive patient data.

1. **Anomaly Detection and Threat Identification**: AI and ML can analyse data, identify patterns, and detect unusual with a remarkable degree of accuracy. In the context of PHI, these technologies can monitor activity logs and usage patterns to spot actions that deviate from the norm, potentially indicating a security breach or unauthorised access. Since AI systems operate on data, their accuracy continues to improve, enhancing their ability to identify threats proficiently.
2. **Predictive Analytics for Proactive Security**: AI can strengthen IT security by proactively identifying threats before they materialise. By utilising real--world data, AI systems can highlight potential risks and propose courses of action. For instance, if an AI system detects an increase in phishing

attempts targeting healthcare professionals, it may notify administrators to tighten email controls and organise awareness sessions.

3. **Automated Compliance Monitoring**: By incorporating AI and ML into the healthcare sector, organisations can more effectively oversee compliance obligations. These technologies can analyse large datasets to identify compliance gaps and generate real-time reports, helping organizations avoid penalties and maintain trust.[7]
4. **Enhanced Data Encryption and De-Identification**: With the help of AI, encryption can be optimised and fine-tuned to secure PHI more effectively. Furthermore, ML can support data de-identification by removing sensitive personal information while retaining data for research or analysis. This facilitates the lawful use of data for secondary purposes without requiring a full consent process from patients.
5. **Natural Language Processing (NLP)**: NLP, a subset of AI, can protect PHI by analysing text data for sensitive information. Specialised NLP algorithms can also perform automated masking or redaction of PHI within medical text, ensuring that only information relevant to a specific purpose is revealed while patients' identities remain concealed.
6. **Robust Access Control Mechanisms**: AI can improve access control systems through biometric identity verification methods and real-time security risk assessment. For instance, AI can employ methods like facial recognition to ensure that only authorised personnel gain access to patient health information.
7. **Challenges and Limitations**: While AI and ML do offer advanced capabilities for PHI protection, they come with significant limitations. These include potential biases in algorithmic decision-making, high implementation costs, and the need for large amounts of high-quality data to train models effectively. Additionally, the "black box" nature of some AI systems raises concerns regarding transparency and accountability, especially in critical healthcare settings.

Homomorphic Encryption

Homomorphic encryption is an advanced cryptographic method that allows computations to be performed directly on encrypted data without first decrypting these data. For this reason, homomorphic encryption is particularly valuable for

[7] *What Is HIPAA Compliance? The Ultimate Guide To Becoming HIPAA Compliant in 2022*. Available from: https://www.easyllama.com/blog/what-is-hipaa-compliance (accessed: 15.07.2024).

 DOI: 10.7206/kp.2080-1084.817

protecting PHI in various healthcare settings, as it enables data processing while keeping the underlying information concealed.

1. **Secure Data Processing**: Homomorphic encryption enables computational analysis of large datasets that remain encrypted, ensuring that the data does not fall into the wrong hands while still allowing healthcare providers and researchers to work with PHI-derived information. For instance, when diagnosing illnesses or diseases, doctors and medical researchers can perform pattern recognition on data concerning specific patient populations without ever needing to see the actual records, thereby preserving each individual's privacy.
2. **Privacy-Preserving Data Sharing**: A major challenge in data exchange is that PHI often needs to be shared between multiple entities, including hospitals, research institutions, and insurance companies. Homomorphic encryption enables secure data sharing by allowing encrypted data to be jointly processed without being exposed or readable. This means that a healthcare provider handling patient data can outsource computational tasks to external services without violating patient privacy rights.
3. **Compliance with Regulatory Standards**: Regulations such as HIPAA and the GDPR mandate strict privacy and security requirements for handling PHI. Homomorphic encryption effectively addresses data-protection concerns and thus assists healthcare organisations in meeting these regulatory obligations. Since data remain encrypted throughout both processing and post-processing stages, the risk of external interference or data breaches is significantly reduced, which is essential for fulfilling legal requirements and securing sensitive health information.
4. **Enhanced Data Security**: Conventional cryptographic techniques require information to be decrypted before it can be processed, exposing potential vulnerabilities during decryption stage. Homomorphic encryption eliminates this risk by ensuring end-to-end encryption. This constant protection substantially reduces the attack surface, making it far more difficult for hackers to access PHI.
5. **Real-World Applications**: Real-world uses of homomorphic encryption in healthcare include secure genomics processing, encrypted medical image analysis, and secure management of patient records. For example, in genomic research, algorithms can analyse encrypted genomic sequences to detect mutations or disease markers without decrypting the data, thereby preserving patient privacy.

6. **Challenges and Limitations**: Homomorphic encryption has several limitations, including high computational demands and considerable complexity. Encryption, decryption, and encrypted computations may require significantly more time and processing power than conventional methods. However, ongoing developments continue to improve performance and scalability.

Regulatory Compliance and Standards

Key Regulations and Frameworks

1. **Health Insurance Portability and Accountability Act (HIPAA)**
HIPAA is one of the most extensive regulatory frameworks governing the handling of PHI in the United States. The Health Insurance Portability and Accountability Act is federal legislation passed in 1996 to establish standards for the confidentiality of health information.

- **Privacy Rule**: The Privacy Rule sets the requirements for the use and disclosure of Protected Health Information. It establishes patients' rights concerning their health information, including the right to access their records and receive copies from their healthcare providers.
- **Security Rule**: The Security Rule prescribes measures that healthcare entities must adopt to protect electronic Protected Health Information (ePHI). These regulatory requirements include the implementation of administrative, physical, and technical measures to protect ePHI from unauthorised access, maintain its confidentiality and integrity, and ensure that the information is available when needed.
- **Breach Notification Rule**: This rule requires covered entities to notify individuals, the Department of Health and Human Services (HHS), and, in some cases, the media in the event of a breach of PHI.

2. **General Data Protection Regulation (GDPR)**
The GDPR, implemented in the European Union in 2018, has significant implications for personal data and, in particular, health data.

- **Data Protection Principles**: The GDPR sets out principles such as purpose limitation, data minimisation, accuracy, storage limitation, and the integrity and confidentiality of personal data.
- **Consent**: GDPR requires explicit consent for the processing of personal information, including health data, and includes provisions for the withdrawal of consent.

 DOI: 10.7206/kp.2080-1084.817

- **Rights of Data Subjects**: Individuals are granted enhanced rights under the GDPR; for example, they may request copies of their data, exercise the right to be forgotten, and invoke the right to data portability.[8]
- **Data Breach Notification**: Organisations are required to report data breaches to the competent authorities within 72 hours of becoming aware of them and to inform affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms[9].

3. Other International Standards and Regulations

- Personal Information Protection and Electronic Documents Act (PIPEDA): In Canada, PIPEDA governs the collection, use, and disclosure of personal information in commercial activities, including health information.[10]
- ISO/IEC 27001: This international standard defines the implementation of an organisational Information Security Management System (ISMS) to protect PHI and maintain a structured and continuously improved security framework.[11]
- Health Level Seven (HL7): HL7 provides a set of international standards for the exchange, integration, sharing, and retrieval of electronic health information, ensuring interoperability and confidentiality of health data.[12]

Compliance Strategies and Best Practices

Strategy	Description
Risk Assessment and Management	Periodic threat assessments and mitigation planning.
Data Encryption and Access Controls	Encrypt data in transit and at rest, implement role-based access controls (RBAC).
Employee Training and Awareness	Training on compliance requirements and recognising security threats.
Incident Response Planning	Structured plans for rapid response to data breaches.
Audit and Compliance Monitoring	Regular audits and continuous monitoring to ensure legal compliance.

8 G. Canto Moniz, *The risk-based approach in the GDPR and the "two-step test" within Article 44*, "International Data Privacy Law" 2024, 14(2), pp. 169–176.

9 L. Bachňáková Rózenfeldová, P. Sokol, R. Hučková, M. Mesarčík, *Personal data protection enforcement under GDPR–the Slovak experience*, "International Data Privacy Law" 2024, 14(3), pp. 278–297.

10 L. Drechsler, H. Matsumi ("Yuki"), *Caught in the middle: The Japanese approach to international personal data flows*, "International Data Privacy Law" 2024, 14(2), pp. 177–185.

11 J. Conde, D. Jerker B Svantesson, *The Five Generations of Facial Recognition Usage and the Australian Privacy Law*, "International Data Privacy Law" 2024, 14(3), pp. 247–258.

12 F. Li, Y. Lin, *A legal-spatial analysis of personal information protection in China's live court trial broadcasts*, "International Data Privacy Law" 2024, 14(3), pp. 259–277.

1. **Risk Assessment and Management**
   It is necessary to conduct risk analyses periodically to identify threats that may compromise effective PHI management. This involves assessing existing threats, analysing their potential consequences for the organisation, and putting in place measures to counter them when necessary. Risk management assists in maintaining appropriate controls and adapting to evolving threats.
2. **Data Encryption and Access Controls**
   One common best practice is ensuring that data are encrypted both at rest and in transit to protect PHI. Access controls, including multi-factor authentication and role-based access, ensure that only authorised personnel can access sensitive information. Such steps assist in reducing the likelihood of unauthorised access and data breaches.
3. **Employee Training and Awareness**
   Another critical area of training is providing employees with regular training, including refresher courses on compliance with data-protection requirements and organisational security procedures. Employees must be aware of their roles and responsibilities related to PHI. Training should include recognising phishing attacks, incident reporting, and appropriate protective measures.
4. **Incident Response Planning**
   It is paramount that the organisation maintains a sound incident response plan capable of responding to any data breach or loss as quickly as possible to reduce its effects. In addition to preventive protocols, the plan should contain procedures for managing violations, including notifications to affected individuals and relevant regulatory bodies.
5. **Audit and Compliance Monitoring**
   Regular auditing and compliance checks are essential for ensuring adherence to legal and organisational standards. This includes verifying that all policies and procedures implemented by the organisation comply with the law, conducting internal and external audits, and providing ongoing training. Continuous system monitoring is necessary to identify and address potential compliance issues.[13]

[13] F. Jalundhwala, V. Londhe, *A systematic review on implementing operational excellence as a strategy to ensure regulatory compliance: A roadmap for Indian pharmaceutical industry*, "International Journal of Lean Six Sigma" 2023, 14(4), p. 730.

 DOI: 10.7206/kp.2080-1084.817

Case Studies and Practical Applications: Real-World Examples of Emerging Technologies in PHI Protection

The privacy of Protected Health Information (PHI) has become increasingly dependent on cutting-edge solutions that preserve health data from leaks, unauthorised access, and intrusion. The following examples illustrate how emerging technologies are being employed to enhance PHI protection in real-world settings:

1. **Blockchain Technology**
   A blockchain-based digital health record and management system, MedRec, has been developed by MIT.[14] It builds on the key characteristics of blockchain technology, which are decentralisation and immutability,[15] enabling records to be stored in a form that cannot be altered. Its importance lies in enabling encrypted sharing of both patient and provider data, particularly medical histories, thereby preventing individuals with malicious intent from altering or accessing information in an unauthorised manner.[16] Blockchain ensures that all access to PHI is logged transparently, enhancing accountability and trust.
2. **Artificial Intelligence (AI) and Machine Learning (ML)**
   Zebra Medical Vision has adopted AI algorithms to analyse a wide range of medical imaging data. In diagnosing diseases, the platform leverages AI while protecting patient privacy by routing data through predefined modules within encrypted and secure networks, allowing for anomaly detection without exposing PHI. AI also strengthens cybersecurity by identifying risks and threats through predictive analytics.[17]
3. **Federated Learning**
   Google has employed federated learning to train ML models across multiple hospitals without requiring the sharing of patient data. In this approach, data remain local to each institution while only model updates are aggregated centrally. This enhances data security because no sensitive health

---

14 A. Ekblaw, A. Azaria, *MedRec: Medical data management on the blockchain*, "Viral Communications" 2016. Available from: https://viral.media.mit.edu/pub/medrec/release/1 (accessed: 15.07.2024).

15 H. Taherdoost, *Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives*, "Sci" 2023, 5(4), p. 41.

16 P. Zhuang, T. Zamir, H. Liang, *Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey*, "IEEE Transactions on Industrial Informatics" 2021, 17(1), pp. 3–19.

17 B. Geluvaraj, P.M. Satwik, T.A. Ashok Kumar, *The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace*, [in:] S. Smys, R. Bestak, J.Z. Chen, I. Kotuliak (eds.), *International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies*, vol. 15. Springer, Singapore 2019, p. 739.

data are transferred between locations, thereby reducing the risk of data breach.[18]

4. **Homomorphic Encryption**
   IBM is at the forefront of exploring the use of fully homomorphic encryption (FHE) to process data while it remains encrypted. For instance, healthcare providers can perform complex analytics on encrypted PHI to derive insights without decrypting the data.[19] This ensures that unauthorised individuals cannot access sensitive information at any stage of the data--processing pipeline, thereby guaranteeing a high level of security.
5. **Zero-Knowledge Proofs (ZKPs)**
   Zero-Knowledge Proofs (ZKPs) have been used by genetic research groups to share genomic data securely. Using this method, researchers can verify whether a genome possesses certain traits without revealing the underlying genetic sequence. This approach promotes collaborative research while maintaining the confidentiality of individuals' genetic information.
6. **Differential Privacy**
   Apple utilises differential privacy to preserve user data privacy while still collecting information that can help improve service delivery. In the healthcare context, differential privacy allows large-scale research and analysis to be conducted without enabling the re-identification of individual patients, thereby maintaining robust privacy protection measures.[20]
7. **Secure Multi-Party Computation (SMPC)**
   Sharemind is one of the successful platforms incorporating SMPC to enable secure computation across data held by different organisations.[21] This method makes it possible for multiple entities to jointly analyse patient data for research purposes without compromising or revealing any individual's information. This preserves data privacy while supporting collaboration between healthcare organisations.[22]

---

18 M. Alazab *et al.*, *Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions*, "IEEE Transactions on Industrial Informatics" 2022, 18(5), p. 3501.

19 V. Biksham, D. Vasumathi, *Homomorphic Encryption Techniques for Securing Data in Cloud Computing: A Survey*, "International Journal of Computer Applications" 2017, 160(6).

20 *What Is Differential Privacy? – MIT Ethical Technology Initiative*. Available from: http://eti.mit.edu/what-is-differential-privacy (accessed: 16.07.2024).

21 *Overview: Sharemind Developer Zone*. Available from: https://docs.sharemind.cyber.ee/sharemind-mpc/2023.09/prologue/overview.html (accessed: 16.07.2024).

22 R. Dang-Awan, J.A. Piscos, R.B. Chua, *Using ShareMind as a Tool to Develop an Internet Voting System with Secure Multiparty Computation*, 2018, 9th International Conference on Information, Intelligence, Systems and Applications, IISA 2018.

 DOI: 10.7206/kp.2080-1084.817

Conclusion

Protecting PHI in the modern world involves the use of technologies combined with adherence to relevant legislation and the principles of ethical conduct. Healthcare is a rapidly growing industry that faces daily challenges in maintaining patients' data privacy, trust, and PHI security. It is essential that this sector invest in newer technological solutions such as blockchain, artificial intelligence, and advanced encryption methods for secure data protection. Organisations should also take into consideration regulatory requirements such as HIPAA, the GDPR, and the DPDP to ensure that any legal issues are addressed appropriately.

It is imperative that patients' ethical rights are protected and upheld with openness, fairness, and data integrity. Greater collaboration, whereby government authorities work alongside industry experts, can help bridge existing gaps and strengthen PHI protection. Cross-sector cooperation can also aid in safeguarding patients' health data. Modern healthcare is increasingly digitised and encompasses a wider range of personal information. Hence, blockchain technology offers a reliable and secure framework for preventing unauthorised access and ensuring robust access control.

Key Findings

The research project reveals critical gaps in the protection of Protected Health Information (PHI) within the healthcare sector. While regulations such as the DPDP Act 2023 provide a legal framework for data protection, the legislation is not specifically tailored to health data, and healthcare institutions therefore struggle with compliance. There is also inadequate cybersecurity infrastructure, insufficient training and limited awareness of emerging data-protection laws. The study also finds that, while Electronic Health Records (EHRs) improve healthcare efficiency, they also pose significant risks of data breaches if not properly managed. Moreover, disparities in the enforcement of data protection laws across regions result in inconsistent PHI security, emphasising the need for a more unified approach to healthcare data privacy. On the positive side, the article highlights the significance of emerging technologies for PHI protection. These technologies are considered reliable and suitable for wider adoption to enhance the level of PHI security.

References

Alazab M., RM S.P., P.M, Maddikunta P.K.R., Gadekallu T.R., Pham Q.-V., *Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions*, "IEEE Transactions on Industrial Informatics" 2022, 18(5), pp. 3501–3509. https://doi.org/10.1109/TII.2021.3119038

Bachňáková Rózenfeldová L., Sokol P., Hučková R., Mesarčík M., *Personal data protection enforcement under GDPR–the Slovak experience*, "International Data Privacy Law" 2024, 14(3), pp. 278–297. https://doi.org/10.1093/idpl/ipae008

Biksham V., Vasumathi D., *Homomorphic Encryption Techniques for Securing Data in Cloud Computing: A Survey*, "International Journal of Computer Applications" 2017, 160(6). https://doi.org/10.5120/ijca2017913063

Canto Moniz G., *The risk-based approach in the GDPR and the "two-step test" within Article 44*, "International Data Privacy Law" 2024, 14(2), pp. 169–176. https://doi.org/10.1093/idpl/ipae006

Conde J., Jerker B Svantesson D., *The five generations of facial recognition usage and the Australian privacy law*, "*International Data Privacy Law"* 2024, 14(3), pp. 247–258. https://doi.org/10.1093/idpl/ipae007

Dang-Awan R., Piscos J.A., Chua R.B., *Using ShareMind as a Tool to Develop an Internet Voting System with Secure Multiparty Computation*, 9th International Conference on Information, Intelligence, Systems and Applications, IISA 2018. https://doi.org/10.1109/IISA.2018.8633690

Drechsler L., Matsumi H. ("Yuki"), *Caught in the middle: The Japanese approach to international personal data flows*, "International Data Privacy Law" 2024, 14(2), pp. 177–185.

Ekblaw A., Azaria A., *MedRec: Medical data management on the blockchain*, "Viral Communications" 2016. Available from: https://viral.media.mit.edu/pub/medrec/release/1 (accessed: 15.07.2024).

Geluvaraj B., Satwik P.M., Ashok Kumar T.A., *The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace*, [in:] S. Smys, R. Bestak, J.Z. Chen, I. Kotuliak (eds.), *International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies*, vol. 15. Springer, Singapore 2019. https://doi.org/10.1007/978-981-10-8681-6_67

Jalundhwala F., Londhe V., *A systematic review on implementing operational excellence as a strategy to ensure regulatory compliance: A roadmap for Indian pharmaceutical industry*, "International Journal of Lean Six Sigma" 2023, 14(4), pp. 730–754. https://doi.org/10.1108/IJLSS-04-2022-0078

Li F., Lin Y., *A legal-spatial analysis of personal information protection in China's live court trial broadcasts*, "International Data Privacy Law" 2024, 14(3), pp. 259–277. https://doi.org/10.1093/idpl/ipae009

Lincke S., *Planning for Network Security*, [in:] *Information Security Planning*. Springer, Cham 2024. https://doi.org/10.1007/978-3-031-43118-0_8

Overview: Sharemind Developer Zone. Available from: https://docs.sharemind.cyber.ee/sharemind-mpc/2023.09/prologue/overview.html (accessed: 16.07.2024).

Taherdoost H., *Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives*, "Sci" 2023, 5(4). https://doi.org/10.3390/sci5040041

What Is Differential Privacy? – MIT Ethical Technology Initiative. Available from: http://eti.mit.edu/what-is-differential-privacy (accessed: 16.07.2024).

What Is HIPAA Compliance? The Ultimate Guide To Becoming HIPAA Compliant in 2022. Available from: https://www.easyllama.com/blog/what-is-hipaa-compliance (accessed: 15.07.2024).

Zhuang P., Zamir T., Liang H., *Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey*, "IEEE Transactions on Industrial Informatics" 2021, 17(1), pp. 3–19. https://doi.org/10.1109/TII.2020.2998479