IAA Journal of Biological Sciences 13(1):109-115, 2025
©IAAJOURNALS
https://doi.org/10.59298/IAAJB/2025/131109115
www.iaajournals.org
ISSN:2636-7254
IAAJB131

Data Privacy in Health Informatics: Engineering Secure Systems

Omeye Francis I.

Faculty of Medicine Kampala International University Uganda

ABSTRACT

Health Informatics is revolutionizing how patient data is collected, managed, and utilized to enhance the quality of care and public health outcomes. However, as digital systems become more integrated into healthcare, concerns over data privacy and security intensify. This paper examines the multidimensional aspects of data privacy in health informatics, from legal regulations to technical safeguards, including encryption, access control, anonymization, and secure system design. It discusses the balance between data utility and privacy protection, identifies threats such as inference and linkage attacks, and underscores the importance of risk assessment and management. The study also explores how hospitals implement electronic-based systems and privacy frameworks, with emphasis on European practices. Drawing from best practices, regulatory standards like GDPR and HIPAA, and technological innovations, this research outlines engineering principles for secure health information systems. The paper concludes that privacy-by-design and continuous risk management are essential to foster public trust and ensure ethical use of health data in modern healthcare ecosystems.

Keywords: Health Informatics, Data Privacy, Secure Systems, Electronic Health Records (EHR), GDPR, HIPAA, Anonymization, Data Encryption.

INTRODUCTION

Health Informatics is a multidisciplinary field that integrates Information Science, Computer Science, and Health Care to improve the organization and usage of health information. Its goal is to enhance care quality by ensuring timely access to comprehensive and relevant data, involving the acquisition, storage, analysis, and communication of health information. This domain includes not just software systems but also services and processes that support health professionals in decision-making and health policy development. As populations age and healthcare needs grow amidst limited resources, Health Informatics offers a global framework to reorganize healthcare systems. Countries are increasingly spending more on healthcare, yet budget cuts lead to declining system effectiveness. Managing larger, complex data sets requires greater effort from health professionals to derive meaningful insights for societal advancement. Modern Health Informatics Systems use intelligent information systems that can handle complexity, analyze real-time data, enhance research, support patient autonomy, and improve care. Ensuring privacy and security within this sensitive field is crucial, as Health Informatics can provide a competitive edge for organizations, though it can also lead to privacy oversights. Therefore, secure Health Informatics Systems must be developed with robust security measures integrated from the design phase, illustrating that secure systems are effective in protecting users and sensitive information [1, 2].

Importance of Data Privacy

With advancements in data-driven technologies, big data analytics have become essential in various sectors, especially health informatics. This field utilizes computer and data science techniques to enhance understanding of health and disease, making significant strides in both theory and practical biomedical data systems. An effective data-driven healthcare system can improve patient monitoring and clinical treatment effectiveness. However, this progress necessitates exceptional efforts to safeguard patients' health privacy and personal information while maintaining data utility. Protecting health data privacy is critical due to the sensitivity of the information involved. Unauthorized exposure of health data violates HIPAA requirements and can have serious lifelong consequences for patients. Healthcare teams have access to this data, while researchers and companies often seek it for studies, creating tension due to the lucrative opportunities in healthcare big data versus the risks to patient privacy. Balancing data utility and analytic model learning is challenging when deploying practical analytics systems. A common approach to safeguarding IoT/cloud healthcare data privacy involves selecting appropriate methods first, then designing compatible privacy-preserving analytic models. While effective, this approach requires stringent standards for both data protection methods and privacy-preserving algorithms, establishing a trade-off between utility and security. Achieving an ideal balance in privacy protection is nearly impossible; strong protections may impair service performance, while lax protections can be insufficient against breaches. Thus, the significance of each privacy protection method is paramount. [3, 4].

Legal Frameworks and Regulations

Privacy is an important concern in any research programme that deals with personal medical data. Ethics and privacy have become key considerations when conducting any form of scientific research that involves personal data. These issues are now addressed in professional healthcare training programmes. However, these programmes do not deal specifically with the legal framework or the procedures that apply to research involving medical data. For such research to be valid, the data must have been collected by health care professionals, either in a medical treatment or a health data collection context. Therefore, such data are medical data and have a high level of protection. This paper aims to give an overview of the main privacy and data protection issues that researchers need to take into account while working with health data. Several scenarios for electronic health data (EHD) use for research purposes can be distinguished, each of which gives rise to different related data protection considerations. Electronic health data are by definition personal data and as such covered by general data protection laws such as the European Union GDPR and its country-specific implementations. These regulations also include rights for data subjects (patients) and obligations for healthcare providers and other data controllers. Depending on the local regulations, some of these activities might require the establishment of a data protection authority. Additionally, the possibility of wide-ranging data analysis over decentralized databases while still allowing data privacy raises the question of the legal framework governing such data. This necessitates training of the network with such diverse data, thus bringing to the fore the need to find solutions to such legal challenges. The distribution of data used for training such algorithms can, by itself, be a source of bias, raising some ethical concerns [5, 6].

Threats to Data Privacy

Attacks on EHR health data shared for analysis can lead to the identification of individual patients due to patient IDs and diagnosis codes included in public databases, threatening privacy. Modern healthcare applications and networked devices risk consumer data security, making effective solutions for protecting health data in cloud infrastructures essential. Electronic Health Records (EHRs) can enhance healthcare quality and research, but raise privacy concerns. Cloud computing is integral to these technologies, and health data used in studies may expose private records of millions, increasing the risk of inference attacks that leverage background knowledge. Electronic tagging systems may reveal sensitive consumer habits, while exaggerated online narratives can provoke public concern. To promote health information technology adoption, governments have invested heavily in health IT reform. Patients have rights concerning their Personal Health Records (PHRs), including access and modification; however, insufficient de-identification leads to privacy risks and stricter regulations on data use by hospitals, providers, and researchers. PHR systems require careful collection and processing of sensitive health information, necessitating robust privacy measures. Current research emphasizes data confidentiality but overlooks threats like attribute linkage attacks, data correlation attacks, and membership inference attacks [7, 8].

Data Encryption Techniques

To enhance data access restriction and create a secure health informatics environment, Fingerprint Technology is designed so that only trained personnel can operate it. A primary goal is to implement a multi-layered protection architecture, adopting digital rights management (DRM) to ensure material data is accessed solely through secured systems. The DRM must feature a multi-layered architecture, incorporating a Reuters integrating agency with distributed databases, where subscribing users register with parameters like job specifications, audio/visual qualifications, and market research. This necessitates agents signing contracts that include a clause against unauthorized data sharing, potentially leading to damages exceeding 20,000 jewels. The adaptive system maintains integrity through secure databases protected by encryption algorithms. The second layer catalogues the use of acquired materials, detailing publication and propagation specifics with automated commands querying relay-based networks. The primary aim of a permission encryption algorithm is to complicate the decoding of protected materials. High-value materials, stored via encryption, are only distributable by licensed agencies, as misuse by unlicensed ones could lead to security breaches with traceable evidence. With the variety of current hardware devices, Fingerprint Technology must also incorporate behavioral identification as an additional method of security [9, 10].

Access Control Mechanisms

Access control checks if a user can access resources by asking questions like who is trying to access what, the purpose of the request, the user's permissions, and the status of the object. If a user answers positively, they gain access, and log records are created to track who accessed which resources and their actions. These inquiries shape access control policies and mechanisms, which are critical in healthcare for protecting Electronic Medical Records (EMR). Hospital administrators aim to manage EMR access, allowing, for instance, a nurse to oversee patient record access. Implementing and revising access control policies involves various mechanisms and the participation of healthcare authorities and patients. Patients participate in evaluating these policies, leading to the development of different access control models. This study aims to incorporate feedback from healthcare professionals and patients to enhance access control to minimize EMR barriers. They can provide insights into what information is needed, who should access it, the conditions for access, and the user's intentions. Focusing on human processes and needs, this project is a part of the EU IST-FP6 initiative, EMERALD, which aims to assess the accessibility and usability of electronic medical records in healthcare settings [11, 12].

Data Anonymization Strategies

The growing volume of health data and new technologies improve health care through health informatics, bridging the data-software-hardware gap. This text presents a framework for engineering steps in this process. To engineer secure systems, methods from compliance research and biologically inspired techniques must be adapted. Developing anonymization processes to render data usable while protecting privacy is crucial. In the past decade, the volume of health data has increased exponentially, with research areas like data mining and artificial intelligence leveraging this information to enhance healthcare. Patient information brings privacy concerns; thus, data must be anonymized before deploying learning algorithms to prevent data leaks that compromise results' privacy. The anonymization process needs careful engineering. Predictions indicate that by the end of 2020, a significant number of healthcare organizations will implement full-scale visual analytics of diverse data sources to derive metrics aiding decision-making. Organizations must uphold compliance with national regulations and ethical standards, ensuring accountability for patient-impacting decisions. Health informatics centers on sorting problems, necessitating tailored processes to uncover optimal solutions, revisiting confidentiality, security, and usability relationships regarding health data. Exemplar software adaptations must meet security proofs and secure computation needs. Anonymization techniques can be implemented as software modules to protect user privacy, yet some users remain hesitant to share even anonymized data. Methods vary concerning secure operations among data holders and intermediate agents. The first set operates at data holders, managing the public data exchange function, while the second requires an intermediate trusted agent, potentially needing secure hardware to prevent temporal data leakage. Only these latter methods permit parallel data processing for privacy preservation. Recent work has focused on client AI-based numeric classifiers [13, 14].

Secure System Design Principles

There have been many discussions about Secure System Design Principles, also known as Secure System Design Methodologies, based on best practices from industry experience. Some formal methodologies exist, though it's unclear how many are widely followed. The most recognized include the Trusted Computer Security Evaluation Criteria and the Common Criteria, with a major goal of considering security needs during system design. These criteria specify desired security features, evaluate design decisions, and offer implementation advice, but have not been as effective due to a lack of motivation and compliance from commercial organizations and governments. Another set of modern guidelines comes from the Secure Software Assurance Forum, organized under four principles of the system development life cycle, addressing requirements, design, coding, testing, maintenance, operations, software, organization, and tool issues. The Global Institute for CyberSecurity Control has also established guidelines aimed at government agencies procuring security measures like encryption and intrusion detection systems for critical infrastructure sectors. These guidelines encourage good system procurement practices and the specification of expertise levels from suppliers, ensuring cost-effective solutions. Lastly, common sense and heuristics in secure system design emphasize rapid responses to security violations, service modularization, and controlled configuration management of system modules [15, 16].

Risk Assessment and Management

Assessing systems for effectiveness in safeguarding protected health information (PHI) is crucial for healthcare organizations, particularly HIPAA-covered entities and business associates. Effective security designs aim to mitigate risks of confidentiality, integrity, or availability breaches through both qualitative and quantitative approaches, using credible methodologies. Security risk assessment standards and guidelines are vital, featured either as design attributes or within assessment checklists. A 2010-2011 Ponemon Institute survey highlighted significant security countermeasure deficiencies in U.S. healthcare, with 90% of organizations experiencing data breaches, and 60% facing severe security incidents. Each breach reportedly cost organizations over $2 million due to low barriers for attackers. The growth of HITECH spurred a transition to cloud services, portable devices, telephony, and the Internet of Things, increasing attack surfaces and complicating HIPAA compliance for many healthcare organizations. Numerous breaches and financial penalties have followed, often exacerbated by high turnover rates among C-suite leaders and insufficient knowledge transfer during Health Informatics implementation. Such challenges underscore the need to address information risks alongside technological adoption [17, 18].

Implementing Secure Health Information Systems

Hospitals have different policy frameworks and mandates affecting the transition toward fully electronic-based systems. Thus, the extent to which policy frameworks and hospitals' accreditation have an impact on IT security and privacy practices is investigated. The electronic-based systems of interest in the present study are EMR systems, PHI sharing systems with partners such as HIE systems, and telehealth systems. Electronic medical records (EMR), personal health information (PHI), health information exchange (HIE) between partners, and telehealth/hospital television were considered for investigation in the study, along with auditing/network scanning, risk analysis, data security/privacy training, mutual agreements, and others. The goal of the study is to provide an overview of how security and privacy practices have been adopted in European hospitals during the transition toward fully electronic-based systems. A quantitative study based on a survey was conducted, targeting hospitals across Europe. Theoretical propositions/hypotheses were developed, and statistical analyses, including ordinal regression, were performed. The findings suggest a general implementation of IT security and privacy practices in the hospitals. More specifically, shorter lengths of hospital existence, higher perceived sophistication and use of new electronic-based systems, and higher accreditation scores are associated with higher use of health information systems, especially sharing systems with third-party providers. Each electronic-based system's delegation of responsibilities is equivalent to risk analysis and mutual agreement practices. For telehealth systems, the extent to which auditing/network scanning is performed appears to vary. The use of electronic medical records (EMR), personal health information (PHI), and health information exchange (HIE) with partners, such as sharing systems with hospitals, appears to be relatively high in hospital use of IT security practices [19, 20].

Emerging Technologies in Health Informatics

Health informatics is an interdisciplinary field blending information science, computer science, and medical informatics, often viewed as its precursor. Variations in national nomenclature indicate different focuses and approaches. Key issues include data privacy, with third-party breaches and cyber-attacks representing significant concerns. Current technologies involve record digitization, data mining, electronic health records, and the interplay of social media with health informatics. Emerging technologies promise transformative changes in data collection, storage, and usage. Potentially disruptive innovations include sensors, extensive datasets, cloud computing, and complex algorithms. Sensors are now capable of collecting vast amounts of data invisibly. Large databases from hospital EMRs, mobile devices, and genomics are emerging, accumulating data amounts surpassing zettabytes. New data types, like social web data that often lack proper identification or medical coding, complicate health-informatics definitions. Cloud systems enable 24/7 access to immense datasets, altering the landscape through commercial 'mailbox' paradigms. Health and chronic diseases are increasingly seen in the context of daily life, challenging traditional biomedical interpretations. The 'mind-senses-see' paradigm suggests a shift in understanding health informatics. This discussion poses further questions rather than providing clear answers and serves as an initial inquiry. Future possibilities may include online diaries, traffic prediction, brand safety nets, and adaptive learning integrating environmental factors and mental states in personalized medicine [21, 22].

Patient Empowerment and Privacy

Electronic health records (EHR) are not only crucial tools for making informed healthcare decisions when it comes to diagnosing and effectively treating patients but also represent a significant advancement in the way patient information is managed and utilized. However, the very accessibility of these records carries with it substantial risks concerning the exposure of sensitive personal information. When critical details are concealed from healthcare providers, it can lead to serious treatment failures, which creates dire and potentially life-threatening consequences for both patients and providers alike. Legal frameworks in place require that varying layers of EHR data be maintained in a meticulous manner, with some data available for public access while other information remains strictly restricted, specifically for crime investigations or other regulated purposes. Most health record data are secured through a variety of structural and technical measures, with access being carefully limited to authorized personnel who have undergone thorough vetting processes. While there are numerous legislative and administrative safeguards implemented to ensure patient privacy and protection, these measures unfortunately do not fully prevent unauthorized disclosures or access by cybercriminals who are continually looking for vulnerabilities to exploit. Alarmingly, recent attacks targeting cloud technologies have sought to exploit such vulnerabilities specifically in EHR privacy protections, which raises pressing concerns for the healthcare sector. Moreover, policies governing EHR differ markedly across various regions, thereby highlighting a plethora of serious concerns that must be addressed adequately. Policymakers now face the critical task of addressing EHR privacy and security comprehensively and must consider the necessity of revising existing policies to ensure they align effectively with modern data analytics and AI practices that are rapidly evolving. It is of utmost importance to contemplate the ease of access to health data, especially in middle-income and least developed countries that are grappling with significant health analytics challenges. Techniques such as anonymization and the generation of synthetic datasets should be prioritized to not only enhance the capability of data usage for secondary purposes but also to significantly bolster data privacy at the same time, making it safer for both providers and patients. This balanced approach is essential for the future of healthcare data management [23, 24].

Future Trends in Data Privacy

Data privacy in health informatics enables patients to securely share personal information without unauthorized third-party access. Patients retain the right to keep medical records confidential, limiting access to a select few. While sharing health data among practitioners is essential, it must be done through electronic health records (EHRs) that maintain patient privacy. Research subjects must remain unidentifiable, ensuring sensitive patient details cannot be inferred from non-sensitive data shared with researchers. Security ensures data is accessible only to essential personnel, but the challenge remains: the question of "where to hide the data" does not fully resolve privacy concerns. A new privacy-preserving health analytics process is needed, utilizing a cross-sharing framework that allows different data holders to collaborate while protecting patient privacy. IoT and cloud-based healthcare systems monitor patients' vital signs through distributed devices, transmitting data to cloud servers for analysis. While effective, these systems raise privacy risks due to sensitive data transmission over the insecure Internet, potentially leading to identity theft and exposure of private health information. Current privacy-preserving solutions in smart healthcare often lack usability, efficiency, and robust security. To address this, a two-phase framework for privacy-preserving secure healthcare analytics is proposed. The first phase involves algorithms that transform data while maintaining its privacy, and the second phase introduces privacy-preserving machine/deep learning algorithms to ensure the cloud server can deliver necessary services without compromising model privacy. Together, these phases protect against both privacy violations and malicious threats [25, 26].

Case Studies in Health Informatics

We highlight essential design rules critical for health informatics research through a thorough examination of three compelling case studies that collectively emphasize the undeniable need for enhanced participatory design practices along with rigorous, systematic evaluations. Our analysis presents a set of well-established design rules derived from both academic literature and practical case studies, aimed at assisting researchers in aligning their work effectively with invaluable existing insights in the field. The tools that we discuss prioritize not only the economic aspects but also the social dimensions inherent in health informatics. Furthermore, the emergence of new technologies has revolutionized the ability to collect extensive volumes of data, leading to the phenomenon frequently described as the “datafication” of health contexts. This transformation fundamentally alters daily life, turning everyday activities into extensive data sources via overt surveillance and constant tracking.

While the utilization of de-identified health data plays a crucial role in supporting epidemiological studies and advancing public health knowledge, its licensing for private use engenders significant concerns about patient consent and privacy rights. This pervasive datafication holds substantial implications for the contemporary landscape of health care, particularly with the continual rise of informatics technologies. The first case study that we analyze in detail elaborates how various economic factors intricately influenced the design and functionality of a mobile app logbook specifically created for children managing type one diabetes. This app was developed by health professionals with the aim of empowering young patients to take a more active role in overseeing their diabetes management. However, a critical examination of the recruitment process for users revealed a significant flaw: participants lacking access to mobile technologies were inadvertently excluded from the opportunity to engage, which highlights a previously unforeseen economic issue that impacts equity in health informatics design. The second case study focuses on a stroke risk assessment tool, where the introduction of new automation technologies raised profound ethical concerns regarding the potential omission of patients from the evaluation process. This situation sparked an essential discourse about the power dynamics that exist between patients and developers, ultimately questioning the ethical responsibilities that developers must uphold in ensuring equitable access and representation in health informatics products [27, 28].

CONCLUSION

The advancement of health informatics holds immense potential for improving patient care, disease research, and healthcare system efficiency. Yet, these benefits are intrinsically tied to how well privacy and security are embedded within health information systems. This paper has shown that while regulations such as GDPR and HIPAA provide essential legal frameworks, their effective implementation depends on secure engineering practices, including encryption, anonymization, access control, and continuous risk assessment. Moreover, emerging technologies like AI and cloud computing add complexity, demanding robust and adaptive security models. Achieving true data privacy in health informatics requires a multidisciplinary approach melding legal compliance, technical innovation, and organizational policy. As healthcare systems become increasingly digitized and interconnected, the imperative for secure, ethical, and privacy-conscious design becomes not only a technical challenge but a societal necessity.

REFERENCES

1. Gashu KD, Guadie HA. Ethics in Public Health Informatics. InPublic Health Informatics: Implementation and Governance in Resource-Limited Settings 2024 Nov 20 (pp. 225-262). Cham: Springer Nature Switzerland. [HTML]
2. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: A systematic literature review. Computers. 2024 Jan 31;13(2):41.
3. Herath HM, Herath HM, Madhusanka BG, Guruge LG. Data protection challenges in the processing of sensitive data. InData Protection: The Wake of AI and Machine Learning 2024 Dec 24 (pp. 155-179). Cham: Springer Nature Switzerland. [HTML]
4. Sargiotis D. Data security and privacy: Protecting sensitive information. InData governance: a guide 2024 Sep 12 (pp. 217-245). Cham: Springer Nature Switzerland.
5. Abernethy A, Adams L, Barrett M, Bechtel C, Brennan P, Butte A, Faulkner J, Fontaine E, Friedhoff S, Halamka J, Howell M. The promise of digital health: then, now, and the future. NAM perspectives. 2022 Jun 27;2022:10-31478. nih.gov
6. Wang Q, Su M, Zhang M, Li R. Integrating digital technologies and public health to fight Covid-19 pandemic: key technologies, applications, challenges and outlook of digital healthcare. International Journal of Environmental Research and Public Health. 2021 Jan;18(11):6053. mdpi.com
7. Herzog NJ, Celik D, Sulaiman RB. Artificial intelligence in healthcare and medical records security. InCybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation 2024 Apr 18 (pp. 35-57). Cham: Springer Nature Switzerland. [HTML]
8. Rele M, Patil D. Securing Patient Confidentiality in EHR Systems: Exploring Robust Privacy and Security Measures. In2023 27th International Computer Science and Engineering Conference (ICSEC) 2023 Sep 14 (pp. 1-6). IEEE. [HTML]
9. Ji T, Li W, Zhu X, Liu M. Survey on indoor fingerprint localization for BLE. In2022 IEEE 6th information technology and mechatronics engineering conference (ITOEC) 2022 Mar 4 (Vol. 6, pp. 129-134). Ieee. [HTML]

10. Liu C, Wang H, Liu M, Li P. Research and analysis of indoor positioning technology. In2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE) 2021 Mar 26 (pp. 1212-1217). IEEE. [HTML]
11. FERREIRAabd A, Ricardo CC, Antunes L, Chadwick D. Access control: how can it improve patients' healthcare?. Medical and care compunetics. 2007 May 31;4(4):65.
12. Abomhara M, Køien GM, Oleshchuk VA, Hamid M. Towards Risk-aware Access Control Framework for Healthcare Information Sharing. InICISSP 2018 Jan (pp. 312-321).
13. Vovk O, Piho G, Ross P. Methods and tools for healthcare data anonymization: a literature review. International Journal of General Systems. 2023 Apr 3;52(3):326-42.
14. Sampaio S, Sousa PR, Martins C, Ferreira A, Antunes L, Cruz-Correia R. Collecting, processing and secondary using personal and (pseudo) anonymized data in smart cities. Applied Sciences. 2023 Mar 16;13(6):3830. mdpi.com
15. Magaji M. Office Ergonomics Awareness and Safety Challenges in Zamfara State Tertiary Institutions. International Journal. 2024 Aug;14(2).
16. Ebad SA. Exploring how to apply secure software design principles. IEEE Access. 2022 Dec 7;10:128983-93.
17. Terry M, Oigiagbe OD. A comprehensive security assessment toolkit for healthcare systems. Colonial Academic Alliance Undergraduate Research Journal. 2015;4(1):6.
18. Habli I, Jia Y, White S, Gabriel G, Lawton T, Sujan M, Tomsett C. Development and piloting of a software tool to facilitate proactive hazard and risk analysis of Health Information Technology. Health informatics journal. 2020 Mar;26(1):683-702.
19. Alfawzan N, Christen M, Spitale G, Biller-Andorno N. Privacy, data sharing, and data security policies of women's mHealth apps: scoping review and content analysis. JMIR mHealth and uHealth. 2022 May 6;10(5):e33735. jmir.org
20. Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Dec 1;1:100016.
21. Arafat MS, Desai K, Hossain MA, Asha AI, Akter S. Cybersecurity Challenges in Healthcare IT: Business Strategies for Mitigating Data Breaches and Enhancing Patient Trust. The American Journal of Engineering and Technology. 2025 May 6;7(05):15-38. inlibrary.uz
22. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.
23. Pai MM, Ganiga R, Pai RM, Sinha RK. Standard electronic health record (EHR) framework for Indian healthcare system. Health Services and Outcomes Research Methodology. 2021 Sep;21(3):339-62. springer.com
24. Zarour M, Alenezi M, Ansari MT, Pandey AK, Ahmad M, Agrawal A, Kumar R, Khan RA. Ensuring data integrity of healthcare information in the era of digital health. Healthcare technology letters. 2021 Jun;8(3):66-77. wiley.com
25. Sharma S, Chen K, Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing. 2018 Jan 16;22(2):42-51.
26. Goldstein ND, Sarwate AD. Privacy, security, and the public health researcher in the era of electronic health record research. Online journal of public health informatics. 2016 Dec 28;8(3):e207.
27. Hassani H, Silva ES. The role of ChatGPT in data science: how ai-assisted conversational interfaces are revolutionizing the field. Big data and cognitive computing. 2023 Mar 27;7(2):62.
28. Beardsley M, Albó L, Aragón P, Hernández-Leo D. Emergency education effects on teacher abilities and motivation to use digital technologies. British Journal of Educational Technology. 2021 Jul;52(4):1455-77. wiley.com

CITE AS: Omeye Francis I. (2025). Data Privacy in Health Informatics: Engineering Secure Systems. IAA Journal of Biological Sciences 13(1):109-115. https://doi.org/10.59298/IAAJB/2025/131109115