European Journal of Applied Sciences – Vol. 13, No. 05
Publication Date: October 28, 2025
DOI:10.14738/aivp.1305.19479.
Onwuegbuchulam, C., Chibu-Obinna, O. U., & Ezebunanwa, A. C. (2025). Precision, Privacy, Protection: The New Triad of Healthcare Data Integrity. *European Journal of Applied Sciences, Vol - 13(05).* 450-459.

Precision, Privacy, Protection: The New Triad of Healthcare Data Integrity

Chukwudi Onwuegbuchulam
Teesside University Middlesbrough
School of computing, engineering, and digital technologies

Onyinye Ugochi Chibu-Obinna
Torrens University, Australia Department of Public Health

Ezebunanwa, A. C.
Hertfordshire University, Hatfield United Kindom
Department of Management Hertfordshire Business School

ABSTRACT

Digital transformation in the healthcare domain has significantly shed light on the question of data integrity and the critical role that the triad of precision, privacy, and protection plays in ensuring data integrity. The paper addresses complex issues, including the need to maintain a structural balance that provides the honest, effective, and ethically justifiable handling of health data. The accuracy of information and its application in clinical practice and research, patient privacy, legal protection of patients, and safeguards against increasing cyber threats. Even with these two foundations of continuously growing data integrity and security, trade-offs between data utility, accessibility, and other aspects remain possible. New and emerging technologies, such as blockchain and privacy-preserving technologies (PPTs), include homomorphic encryption and Federated learning. Data, in turn, is facilitated by such technologies, which enhance the protective layers of privacy and data integrity, but also introduce challenges of scale, interoperability, and an expensive nature, as well as ethical concerns, including algorithmic bias. This paper aims to establish interdisciplinary, open, and data-driven patient processes, including dynamic consent, to foster social trust and social justice, thereby addressing the gaps in scalability, interoperability, and equitable access to digital health technologies. The necessity of creative, data-driven, collaborative, and patient-centered interdisciplinary innovations requires vigilance to maintain the protective integrity of Cardinal Health data.

Keywords: Data integrity, Healthcare, Precision, Privacy Protection, Digital transformation, Blockchain, Federated learning.

INTRODUCTION: THE SIGNIFICANCE OF DATA INTEGRITY IN HEALTHCARE

The healthcare industry is rapidly becoming digitalized as it adopts electronic health records and specialized software. This is in addition to telemedicine and other health applications, as well as artificial intelligence, which now analyzes health data. Such trends in advanced data healthcare are associated with improved diagnosis, better treatment, and research [1]. Healthcare officers are examples of the experts who use EHRs to create patient records. When adhered to, these notes reduce the mistakes that may arise during patient treatment. Now, AI collaborates directly with the healthcare industry and is capable of approximating potential results and even monitoring trends that might require intervention [2,3]. Conversely, identifying the real price of the data, the confidentiality of the patient, and the credibility given to a patient are significant obstacles to success.

The integrity of healthcare data underpins the quality of patient care. Data integrity implies that data are reviewed and validated to ensure they cannot be contested, disagreed with, and are entirely accessible, unbiased, and accurate [4]. With poor integrity being looked down upon or regarded as something unworthy of being maintained, the implications are terrible. These involve misdiagnosis, mistreatment, unnoticed malfeasance, violation of confidentiality, and the loss of trust and goodwill of the patient being maligned [5]. Enhancing data management practices has become a priority following high-profile instances of ransomware attacks on hospitals, which have resulted in the theft of sensitive patient information [6]. Additionally, the increased focus on the secondary use of data, such as research or community health surveillance, underscores the importance of effective data management and data stewardship practices [7].

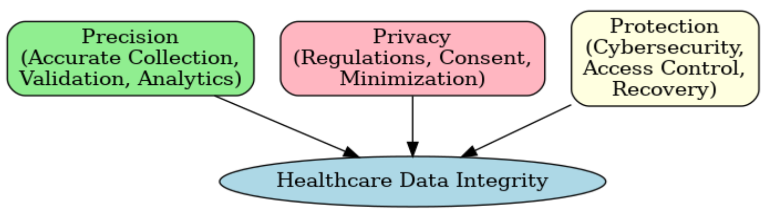

Figure 1: The Triad Model of Healthcare Data Integrity

These challenges, together with the principles of accuracy, confidentiality, and security, have become the foundation of healthcare data integrity.

- **Precision** involves careful collection, validation, and verification of medical information, ensuring that decisions at both the clinical and operational levels are based on accurate and dependable evidence [8].
- **Privacy** is about reducing the risk of exposing sensitive patient information. It is safeguarded through legal and ethical frameworks such as HIPAA (Health Insurance Portability and Accountability Act) and the GDPR (General Data Protection Regulation) [9,10].
- **Protection** refers to the organizational and technical measures designed to guard healthcare data against breaches, unauthorized access, and cyberattacks, ensuring that the information remains secure [11].

It is critical to the three-fold interaction. Take, for example, that precision ensures the data meets its objective, and that privacy and protection guarantee the data remains confidential, with all necessary measures in place. The same can be said about the fact that establishing such a balance is challenging in the context of privacy, as data can only be helpful when it is maintained securely [12].

The paper discusses the role of precision, privacy, and security in ensuring the integrity of medical data in the digital age, which is achieved through a collaboration of these three. The study will present a cohesive solution to various healthcare stakeholders, including healthcare providers, policymakers, and technologists, through the examination of best practices, current challenges, and real-life case studies applicable to each area. The long-term objective is to foster a paradigm shift in the existing healthcare data model, which should facilitate a balanced approach to precision, privacy, and protection of healthcare data, thereby maintaining the integrity of healthcare data as a patient, clinician, and societal asset.

PRECISION: THE FOUNDATION OF ACCURATE HEALTHCARE DATA

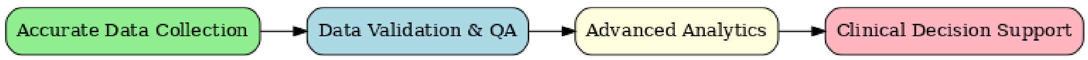

Figure 2: Precision Workflow

Accurate Data Collection

Data collection and data management are inherent elements of healthcare data integrity. The quality of clinical decisions, research, and operational functions depends on the accuracy of the data collected at the point of care. The norms of data collection, including SNOMED CT and LOINC coding systems [1], as well as the list of medical tools and IoT devices, have improved data collection in real-time by allowing clinicians to measure the vital signs of patients and record all activities in clinics automatically, and simplified data entry and management [2]. However, human error, calibration issues with the devices and system silos, and other factors may also impact the accuracy of the gathered data [3]. For instance, inaccurate reporting of a patient's allergies to a specific medicine can be disastrous, which is why more efficient data collection policies need to be formulated [4].

Data Validation and Quality Assurance

Data should always be checked and validated after collection to ensure that the data collected is of high quality. The process of validation can facilitate the automated detection of missing data, gaps, or disproportionate data values, which can lead to the identification of outliers [5]. Monitoring data, particularly in larger systems, becomes crucial. To illustrate, the healthcare systems in general are highly affected by simple mistakes [6]. To minimize these errors and enhance patient care, other systems, such as AI, anomaly detection, or other algorithms and tools, may be utilized. One such application is in the tracking of laboratory results, which helps detect and address patterns before they reach patients [7]. Even with these developments, other organizational constraints, including resource scarcity and the need to keep up with changing data standards, remain obstacles to these organizations [8].

Advanced Analytics and Decision Support

Decision support systems, along with advanced analytics, have transformed the purpose of data within the healthcare ecosystem. Healthcare data is analyzed using Machine Learning (ML) and Artificial Intelligence (AI) algorithms for pattern recognition and prediction of a patient's clinical future, which is utilized in the development of personalized medicine [9]. However, the effectiveness of these tools is directly tied to the precision of the underlying data. Incomplete, biased, and incorrect data can lead to misleading and potentially dangerous diagnoses or inappropriate treatment recommendations [10]. Research has shown that AI models trained on non-representative data often fail to accurately represent minority groups [11]. The efficient use of advanced analytics in healthcare is impossible without data governance as well as the continual improvement of data quality systems [12].

PRIVACY: SECURING SENSITIVE HEALTHCARE INFORMATION

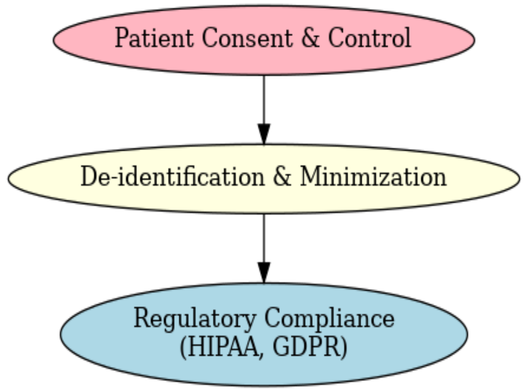

Figure 3: Privacy Safeguards

Regulatory Frameworks and Compliance

Healthcare is a complex industry that is intertwined with business, hence making privacy a highly contested right. The Health Insurance Portability and Accountability Act established national standards and protections for individually identifiable health information in the U.S., and the General Data Protection Regulation imposes its own limitations on data privacy and security in the member states [1] [2]. Healthcare entities today are required to, and as such, are formulating strong policies and technical safeguards to protect patient data, including access controls, audit logs, and deficiency response initiatives [3]. The contradictory legislation, particularly in cases where organizations are involved in multiple jurisdictions [4], such as the GDPR's right to be forgotten versus the Retention of Medical Records law in other states, however, complicates compliance and makes the operation of multinational healthcare businesses challenging [5].

Data Minimization and De-Identification

A healthcare organization can enhance patient privacy by implementing specific data collection and retention policies [6]. These policies ensure that only the information necessary to achieve a given purpose is stored. This reduces the danger of unauthorized disclosure and the possible harm in the event of a serious breach. Anonymization and pseudonymization, which are two de-identification methods, strike a balance between privacy and secondary uses of data for research and public health [7]. The use of de-identified datasets has been helpful in epidemiological and treatment studies. With this as an example, new studies, treatments, and epidemiology studies have progressed in the absence of explicit knowledge in the subjects [8]. The new relevance of the reidentification risk continuum may apply to current developments in external datasets and data analytics [9]. There is an underlying anxiety and a delicate balancing task of ensuring privacy, versus putting data to constructive use [10].

Patient Consent and Control

Allowing patients to have some control over their individual records is a groundbreaking move in terms of privacy. Consent is no longer a mere formality. Thus, patients should be able to consent to the access of their data actively [11] to understand how, where, and by whom it may be accessed. Patient websites and digital health systems provide patients with greater control over their files, enabling them to manage the dissemination of data and restrict unsupervised access to specific researchers [12]. In research areas such as genomic research and biobanking, progressive consent models enable patients to change their minds over time [13]. Nevertheless, the idea of gathering information and/or conducting research depends significantly on the nature of consent. The issues of consent fatigue and varying levels of digital competence, which are accompanied by the constantly growing challenge of deciphering privacy notices, come to mind easily [14]. These impediments to widespread consent must be countered within the realms of lifelong learning, structural responsibility, and relevant inductions [15].

PROTECTION: SAFEGUARDING DATA AGAINST BREACHES AND UNAUTHORIZED ACCESS

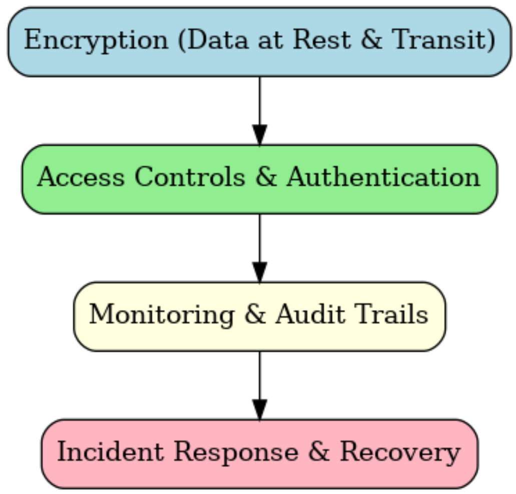

Figure 4: Protection Architecture

Cybersecurity Measures

Cyberattacks have exposed the healthcare sector to significant risks due to the digitization of healthcare information and the integration of health systems [1]. Implementing holistic cyber defence and proactive policies to protect sensitive health data against unauthorized access and malicious attacks is essential. It is necessary to support the encryption of data both during storage and transmission, as well as the adoption of information control systems and fire defence strategies [2]. Maintaining the security of the patient's health and sensitive information about him requires carrying out systematic and regular monitoring of the health organization's internal systems [3]. The vulnerabilities in unsecured patient information monitoring systems expose the organization and the healthcare industry to significant competition, especially after cyberattacks like WannaCry, which struck in 2017 [4]. However, inspections, such as those conducted on Target's patient information systems, enable the organization to take proactive measures against threats and underexploited vulnerabilities [5].

Access Controls and Authentication

A unique characteristic of performing one's job is that the person is given access to role-based access control (RBAC), which is a tested system of access limitation. There is also a type of user verification in the Multi-factor Authentication (MFA) [6]. The audit trails and logging systems help maintain transparency and accountability by capturing the time and identity of the user who accesses or modifies a specific dataset [7]. The most common type of healthcare systems utilizes the known best practices, such as the principle of least privilege, according to which user access is limited to the minimum required [8]. Additionally, there is the issue of insider threats to a system, including unauthorized access, staff abuse, and the declining need to assess training effectiveness [9]. Additionally, there is limited access to timely information, a characteristic of the security required for accessing the information, which poses a challenge, especially in the case of Emergency Care [10].

Incident Response and Recovery

Any security system has its flaws. Thus, incident response and recovery planning play an essential role in securing sensitive healthcare data. Companies must develop and practice a detailed breach response policy to prevent and minimize the harm inflicted by data security breaches [11]. The data retrieval plan, disaster recovery plan, and business continuity plan will help restore functions and minimize the impact on patients [12]. To illustrate, an immediate response to a data breach event can help reduce exposure to sensitive information and mitigate the legal consequences of data breach incidents [13]. Nevertheless, timely identification of violations, proper reaction, and proper reputation management remain to be developed, as all these are of the utmost importance to healthcare organizations [14].

INTEGRATING THE TRIAD: A HOLISTIC APPROACH TO DATA

The interaction of precision, privacy, and protection of healthcare data raises not only technical issues but also various dimensions of these issues, necessitating the consideration of interdependencies and trade-offs, as well as the development of new technological solutions to address these issues. The dilemma of balancing the three dimensions is dealt with in this chapter. This chapter addresses the latest solutions to the problem of data integrity and the unexplored ethical consequences of such solutions on data privacy.

Interdependencies and Trade-offs

The triad of technological and legal precision, privacy, and safety of healthcare data is complicated and, at times, contradictory, yet essential. The accuracy of data is imperative for making clinically informed decisions, implementing personalized medicine, and achieving highly positive outcomes in research. For instance, real-time data capture on wearable devices can be utilized to enhance diagnostic and therapeutic processes through precision medicine. Meanwhile, strict privacy regulations, such as data minimization and de-identification, can reduce the use of secondary data in machine learning population health research [1]. As an illustration, such anonymized datasets can be underrepresented in terms of critical health equity and intervention information, thus limiting their capacity to improve customized health intervention programs. End-to-end encryption, multi-factor authentication, and role-based access controls are essential factors in preventing breaches and cyberattacks on valuable health information. Simultaneously, they may influence access to critical information in time-sensitive scenarios, such as emergencies, where the response time to accessing medical records can be detrimental [2]. In 2023, a study identified instances where access control was implemented conservatively, leading to failures to safeguard lives in trauma wards, and suggested that such approaches demonstrate at least a relative requirement for contextual security, allowing access and closure [10]. In addition, with encryption, the more one processes information, the less computing resources the system will allocate to the economically inefficient data processing rate in the case of a rural data-sparse electronic health record (EHR) system, compared to the amount of data required, and this will cause increased inequity in the information processing of a given requirement.

The defensible solution to such challenges will entail determining which actions can be taken independently and which must be coordinated within a structure to achieve organizational objectives and legislative requirements. Consider the cases of the United States' HIPAA and the European Union's Privacy Act, each with its own privacy and data security limits, but also with boundaries for loosening the stringency of the security standards set, depending on comparative evaluations of the actual security risk presented [3]. As with most operational data issues, these trade-offs will be quantified as a balance between the benefits that the data will likely gain once it is used and the harm that a breach of privacy or security would cause. Such models will frequently be tiered models, in which only authorized access to data is permitted to guard against its misuse, while allowing the misuse of non-sensitive data. For example, masked or de-identified data can be used in research projects with minimal compliance overhead. Conversely, more sensitive and extensive data in clinical environments should be handled with greater care and discretion. These and similar collaborative governance models are becoming a sign of best practice in demonstrating responsiveness to the needs mentioned above. These models bring together various participants, including clinicians, information technologists, lawyers, ethicists, and advocates, to ensure that their decisions encompass clinical needs, technical capabilities, legal factors, and the patient's perspective [4]. For example, patient advisory councils can help identify data uses that foster trust and support the implementation of privacy protection policies that patients expect. Additionally, interdisciplinary teams have the opportunity to develop models of dynamic consent, in which patients can choose to provide their information in real-time for use in research, thereby increasing privacy and enabling multi-use to conduct precision research. These frameworks play a significant role in resolving the ethical and practical issues of the triad, ensuring that the data is reliable and valuable.

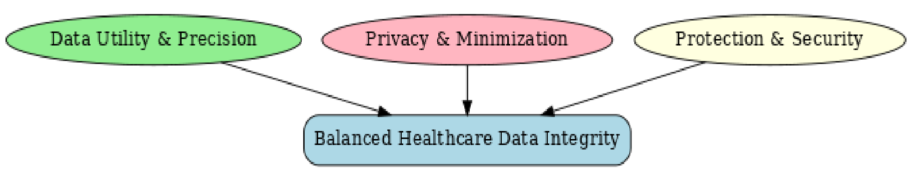

Figure 5: Integration & Trade-offs

Emerging Technologies and Future Directions

Technological advancements are revolutionizing the way healthcare data is handled, incorporating accuracy, confidentiality, and safeguards, while presenting new challenges, as elaborated below.

Blockchain Technology:

Blockchain improves the quality and safety of health records through a distributed and immutable ledger. It reduces the chance of failure at one node and unauthorized alteration of the information, thus maintaining the integrity and verifiability of the records by storing data on a network of nodes [5]. For example, consider blockchain-based systems, such as MedRec, which empower patients by enabling them to manage access to their records using cryptographic keys, thereby enhancing both privacy and accuracy. The scalability of blockchain remains unproven. The blockchain's disintegrated architecture of MedRec may be costly to implement at scale due to the required transactional verification resources. Maintaining legacy systems and blockchain poses interoperability issues that require substantial financing, as well as a considerable effort toward systematization and standardization [8].

Federated Learning:
Federated learning provides a solution to the privacy issue in multi-institutional collaborations, allowing machine learning without the need to share primary patient data. Rather than pooling data, federated learning develops and improves models using the local dataset of each institution and shares only the modified models, thereby upholding privacy and fostering precision medicine initiatives [6]. For example, nearly all federated learning techniques employ collaborative models for predicting rare diseases, which are integrated with data from sensitive patients collected and analyzed at hospitals located in different areas. Nevertheless, such technology requires efficient and reliable infrastructure, which may not be available to smaller or underfunded hospitals, thereby widening the digital health inequality gap. Additionally, with respect to the security of convergence, it is easier to attack not the isolated models, but those produced by combining participant models. The convergence attack is an easier attack to implement, given that adversaries have lower bounds that they are willing to infer, which do not cross sensitive boundaries [11].

Privacy-Enhancing Technologies (PETs):
Homomorphic encryption and secure multi-party computation are one such technology. The methods allow the assessment of the secured data without revealing sensitive information. Picture encryption of a unique identity key enables intricate algorithms to be operated within a firmly secured, shielded environment and yet produce solutions that do not, at any stage, violate these firmly held, invisible boundaries [7]. For example, in the case of encrypted data, hospitals can transparently conduct ciphered patient analytics and decode the obtained data to identify essential health trends without compromising individual privacy or health data security. Equally, different organizations may analyse partitioned datasets together, such as the joint discovery of drugs, without necessarily sharing the underlying primary data. The methods, however, are not hindered without difficulties. The effectiveness of PETs is hindered by several obstacles, including high costs and the additional complexity of the methods compared to less advanced regions. More worrisome, the legal implications of these methods have not been thoroughly addressed, and consequently, none of them can be assured in terms of protection. [8].

Challenges and Ethical Considerations:
It is also essential to address new problems and engage in deeper conversations that can lead to innovative solutions, as learning about complex issues such as ethics and transparency opens new possibilities for improvement. It is significant to develop better solutions, including Investments. Nevertheless, correlative challenges such as long wait times and high health expenditures in developed, health-oriented countries are substantial obstacles both within and outside the medical sector. Reasonable solutions will involve forecasting the amount of money

needed, the amount of funds available, and the capability to rectify any imbalances that may occur.

New information and Blockchain technologies can change the present practice in the healthcare system entirely and predict shifts in the frameworks. The increase in clinical productivity and the decrease in patient equality or in healthcare expenditures are likely to be the focus of ingrained prejudices and moral issues that limit the application of uncontrolled systems under the jurisdiction of healthcare executives [9].

Therefore, resolutions that arise from fairness must be demonstrated to be sustainable. One reason why Blockchain and new technologies are biased and have barriers is that they require freedom. Future research will likely focus on developing affordable solutions to enhance access to wide-area network technology and to address scalability and interoperability issues. In the United States, initiatives such as the National Institutes of Health (NIH) and the European Union, along with public and private collaborations that promote relative equity, have welcomed innovation with the fair allocation of gains. Equally important, the ever-growing intensity of technology in the world necessitates a re-evaluation of regulatory approaches, whether in terms of describing the principles of blockchain interoperability or in the context of domination and control in the federated learning space. The previous model of precision and privacy, influenced by innovations in the health systems sphere in accordance with the principles of ethical design and intentional implementation, can be transformed into a model of protection through the introduction of new technologies.

CONCLUSION

Data integrity is now a critical factor in the healthcare industry and an indispensable component of digital health, mainly due to the advent of innovations in the field. The balance of the three pillars of the integrity of emerging healthcare data ecosystems is precision, privacy, and data protection. The pillars below provide a feasible mental image of the understanding of the Multi-perspective value- and ethics-based approach. Precision must be exercised when working with individual units of data, which are units of protection. The data capture, cost, and loss within specified limits will determine the effective unit of protection value. A privacy breach, which is an outcome of the inability to integrate the data constellation thoroughly, is a significant failure for patients. The price of a violation and the morality of privacy protection are traded off and interdependent; the presence of a strong moral framework for precision highlights the current age of incessant cyberattacks. Modern geopolitics is characterized by a high degree of power balance, protection, and violation. Ethical data units will be more expensive, and so will units of data that are not ethical; both will have freedom at a net profit. The precise percentage of the triad will be based on the autonomous interaction of data interspaces' sophistication, in which the efficacy of governance of constraints has been unanimously agreed upon. There is also a need for models of collaboration that are not based on healthcare governance to comprehend the interfaces. Real progress depends on developers, policymakers, and patients working together, each bringing a unique perspective on interpreting data. When these groups co-create the rules and guardrails, they link perspectives within and beyond healthcare, aligning decisions and opening clear, consistent pathways.

In this context, everyone must treat data integrity as a shared responsibility. This entails developing interdisciplinary governance frameworks, promoting a culture of transparency and continuous improvement, and empowering patients through meaningful consent and agency. Future research should confront persistent problems such as algorithmic bias, weak interoperability across systems, and unequal access to digital health tools. As the sector evolves, trustworthy storage and strong privacy protections will anchor patient-centered, data-driven care, calling for innovation carried out with vigilance and collaboration.

References

[1] Kruse, C. S., & Beane, A. (2018). Health Information Technology Continues to Show a Positive Effect on Medical Outcomes: A Systematic Review. Journal of Medical Internet Research, 20(2), e41. https://doi.org/10.2196/jmir.8793

[2] Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption. Health Affairs, 36(8), 1415–1422. https://doi.org/10.1377/hlthaff.2016.1651

[3] Rajkomar, A., Oren, E., Chen, K., et al. (2018). Scalable and accurate deep learning with electronic health records. npj Digital Medicine, 1, 18. https://doi.org/10.1038/s41746-018-0029-1

[4] Agrawal, A., & Prabakaran, S. (2020). Big Data in Digital Healthcare: Lessons Learnt and Recommendations for General Practice. Heredity, 124(4), 525–534. https://doi.org/10.1038/s41437-020-0303-2

[5] Bowen, R. A. R., & Smith, J. E. (2021). Data Integrity in the Healthcare Industry: Challenges and Solutions. Journal of Healthcare Information Management

[6] Jiang, J. X., & Bai, G. (2025). Ransomware Attacks and Data Breaches in U.S. Healthcare Systems. JAMA Network Open, 8(5), e2420077.

[7] Kruse, C. S., & Goswamy, R. (2021). Ensuring Data Integrity of Healthcare Information in the Era of Digital Health. Healthcare Informatics Research, 27(2), 93–100. https://doi.org/10.4258/hir.2021.27.2.93

[8] Wang, Y., Kung, L., & Byrd, T. A. (2018). Big Data Analytics: Understanding Its Capabilities and Potential Benefits for Healthcare Organizations. Technological Forecasting and Social Change, 126, 3–13. https://doi.org/10.1016/j.techfore.2015.12.019

[9] Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2023). Health Insurance Portability and Accountability Act. StatPearls. https://www.ncbi.nlm.nih.gov/books/NBK500019/

[10] Meszaros, J., & Ho, C. (2020). Big Data and the GDPR: How Privacy Regulations Are Shaping Healthcare Innovation. Health Affairs Blog.

[11] Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. Journal of Medical Systems, 41(8), 127. https://doi.org/10.1007/s10916-017-0778-4

[12] Raghupathi, W., & Raghupathi, V. (2020). An Overview of Health Analytics. Journal of Health & Medical Informatics