World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Ethical considerations in healthcare IT: A review of data privacy and patient consent issues

Adekunle Oyeyemi Adeniyi [1,*], Jeremiah Olawumi Arowoogun [2], Chioma Anthonia Okolo [3], Rawlings Chidi [4] and Oloruntoba Babawarun [5]

[1] *United Nations Population Fund, Sri Lanka.*
[2] *Bharat Serums and Vaccines Limited Lagos*
[3] *Federal Medical Centre, Asaba, Delta State, Nigeria.*
[4] *Park University, & North Kansas City Hospital, Kansas City, MO United State.*
[5] *Global Future Redemption Empowerment Foundation, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 21(02), 1660–1668

Publication history: Received on 13 January 2024; revised on 20 February 2024; accepted on 22 February 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.2.0593

Abstract

This paper delves into the ethical considerations in healthcare Information Technology (IT), focusing on data privacy and patient consent issues. It explores the intersection of technological advancements in healthcare IT and the ethical imperatives guiding their application, specifically examining challenges in ensuring data privacy and obtaining informed consent amidst the complexities introduced by digital health technologies. Through a review of existing ethical theories, regulatory frameworks, and the implications of artificial intelligence (AI) and big data, the paper highlights technological solutions and policy recommendations to address these ethical challenges. It emphasizes the importance of balancing innovation with ethical considerations to protect patient rights and maintain trust in the healthcare system. The paper advocates for ongoing research and stakeholder engagement to evolve ethical standards aligned with technological advancements in healthcare IT.

Keywords: Healthcare IT; Data Privacy; Patient Consent; Artificial Intelligence; Regulatory Frameworks

1. Introduction

The healthcare landscape has been dramatically transformed by Information Technology (IT) advancements, heralding a new era of efficiency, accessibility, and personalized care. Healthcare IT encompasses a broad range of technologies including electronic health records (EHRs), telemedicine, health information exchanges (HIEs), wearable devices, and artificial intelligence (AI) applications. These innovations have streamlined operations, improved patient outcomes through more informed decision-making, and facilitated a shift towards preventive care and wellness. Moreover, seamlessly collecting, analyzing, and sharing health data has been pivotal in research, public health management, and tackling global health crises, such as pandemics (Char, Abràmoff, & Feudtner, 2020; Safdar, Banja, & Meltzer, 2020).

As healthcare IT continues to evolve, it brings to the fore complex ethical considerations that must be addressed to safeguard patient interests and public trust. Central among these are issues related to data privacy and patient consent. The digitization of health records and the proliferation of digital health services have raised significant concerns about the confidentiality and security of personal health information (Ahmad, Singla, & Giri, 2021; Keshta & Odeh, 2021). Ethical considerations in healthcare IT are not merely academic; they have practical implications for patient rights, the provider-patient relationship, and the integrity of the healthcare system as a whole (Pozgar, 2023; Wilkenfeld & McCarthy, 2020). Ensuring data privacy involves protecting health information from unauthorized access, misuse, or

* Corresponding author: Adekunle Oyeyemi Adeniyi

breaches, which could have devastating consequences for individuals' privacy, dignity, and financial security. Equally important is the issue of patient consent, which revolves around patients' right to be informed about and control the use of their personal health information. This includes understanding how their data will be used, who will access it, and the potential risks and benefits of their participation in digital health services.

This paper aims to provide a comprehensive review of the ethical considerations in healthcare IT, with a specific focus on data privacy and patient consent issues. It seeks to explore the ethical dilemmas posed by the rapid expansion of digital health technologies and the implications for patient rights, privacy, and trust in the healthcare system. This review aims to identify the key ethical challenges, examine the existing frameworks and approaches for addressing these issues, and discuss the gaps and opportunities for future improvements. Importantly, this paper focuses on a broad literature review and theoretical analysis to offer insights into the critical ethical considerations for developing and implementing healthcare IT solutions.

2. Literature Review

2.1. Ethical Theories and Principles in Healthcare

The ethical landscape of healthcare IT is informed by several key ethical theories and principles that serve as a foundation for evaluating and guiding moral conduct in the sector.

Deontology: This theory posits that the morality of an action is based on whether that action itself is right or wrong under a series of rules, rather than based on the consequences of the action. In healthcare IT, deontological ethics would argue for strict adherence to rules protecting patient privacy and data security, irrespective of the potential benefits of breaching those rules (Rawling, 2023).

Utilitarianism: Contrary to deontology, utilitarianism suggests that the best action maximizes utility, typically defined as producing the greatest well-being of the greatest number of people. Applied to healthcare IT, utilitarian ethics might justify using patient data in ways that breach individual privacy if the outcome significantly advances public health or improves healthcare outcomes on a large scale (Byskov, 2020; Chukwuneke & Ezenwugo, 2022).

Autonomy: This principle emphasizes the right of individuals to make informed decisions about their own healthcare, including the control over their personal health information. In healthcare IT, respecting autonomy means ensuring that patients are informed about and consent to how their data is used and shared (Varkey, 2021).

Beneficence: This principle requires that actions should be taken to benefit patients and promote their well-being. Within healthcare IT, this could involve using data to enhance the quality of care, personalizing treatment plans, or improving the accuracy of diagnoses.

Non-maleficence: Often summarized as "do no harm," this principle is crucial in healthcare IT. It entails avoiding harm to patients, which includes preventing data breaches that could expose sensitive information and harm the patient in various ways (John & Wu, 2022).

Justice: This principle demands fairness in distributing benefits and risks across the population. In healthcare IT, this means ensuring equitable access to digital health services and ensuring that advancements do not disproportionately benefit or harm specific groups.

2.2. Data Privacy Concepts

In the context of healthcare IT, data privacy is a multi-faceted concept encompassing several critical aspects:

Confidentiality: This refers to the obligation to keep personal health information private, sharing it only with those who need to know how to provide healthcare and with the patient's informed consent. Confidentiality is fundamental in building trust between patients and healthcare providers.

Data Protection: Data protection involves implementing technical and organizational measures to ensure that personal data is processed safely, securely, and in accordance with legal and ethical standards. In healthcare IT, this includes protecting data from unauthorized access, disclosure, alteration, and destruction.

Information Security: Closely related to data protection, information security is specifically concerned with protecting information systems and databases from cyber threats. This includes ensuring patient data's integrity, confidentiality, and availability through various technological means, such as encryption, access controls, and secure data storage and transmission protocols.

Understanding and integrating these ethical theories and principles and a comprehensive approach to data privacy is essential for navigating the ethical challenges in healthcare IT. They provide a framework for evaluating the complex scenarios that arise with digital technologies in healthcare, ensuring that decisions and practices advance healthcare outcomes and respect individuals' rights and dignity.

3. Data Privacy in Healthcare IT

3.1. Challenges of Data Privacy

The integration of Information Technology into healthcare has brought unprecedented benefits, including enhanced patient care, improved efficiency, and the facilitation of medical research. However, it also presents significant challenges to ensuring data privacy, which include:

Technical Vulnerabilities: Healthcare IT systems are complex and often integrate with numerous other systems, creating multiple points of vulnerability. These can include software flaws, outdated systems, and insufficient encryption, which cybercriminals can exploit to gain unauthorized access to sensitive data (Farahani, Firouzi, & Luecking, 2021; Haque, Bhushan, & Dhiman, 2022).

Data Breaches: The healthcare sector is a prime target for data breaches due to health information's valuable and sensitive nature. Data breaches can occur through various means, including hacking, phishing attacks, insider threats, and accidental disclosures. The consequences of such breaches are severe, including financial loss, loss of patient trust, and potential harm to patients' well-being (Almulihi et al., 2022; Zarour et al., 2021).

Unauthorized Access: Unauthorized access to healthcare data can occur from external threats and within an organization. This can be due to inadequate access controls, lack of employee training on data privacy, or intentional misuse by staff. Ensuring that only authorized personnel have access to sensitive information and use it appropriately is a continuous challenge (Patel, 2020).

Mobile and Cloud Technologies: Mobile devices and cloud-based storage have grown in healthcare, offering flexibility and efficiency. However, these technologies also introduce new risks for data privacy, such as loss or theft of devices and a lack of control over where data is stored and how it is secured in the cloud (Javaid et al., 2022).

Interoperability and Data Sharing: While the sharing of health data between providers, researchers, and third parties can improve patient care and advance medical knowledge, it also raises complex privacy issues. Ensuring that data is shared securely and in compliance with patient consent and legal requirements is a significant challenge (Ahmed & Rajput, 2020; Seh et al., 2020).

3.2. Regulatory Frameworks

To address these challenges and protect individuals' privacy, several regulatory frameworks have been established globally:

General Data Protection Regulation (GDPR) in Europe: The GDPR sets stringent data protection standards for the processing of personal data, including health information, of individuals in the European Union (EU) and European Economic Area (EEA). It emphasizes principles like consent, data minimization, and individuals' rights to access and control their data. Healthcare organizations must ensure compliance with GDPR, which includes implementing robust data protection measures, reporting data breaches promptly, and ensuring the lawful processing of health data (Kuner, Bygrave, Docksey, Drechsler, & Tosoni, 2021; Ryngaert & Taylor, 2020; Tamburri, 2020).

Health Insurance Portability and Accountability Act (HIPAA) in the USA: HIPAA provides federal protections for personal health information held by covered entities and gives patients an array of rights concerning that information. It includes the Privacy Rule, which sets standards for the protection of individuals' medical records and other personal health information, and the Security Rule, which sets standards for securing electronic protected health information (ePHI) (Bhate, Ho, & Brodell, 2020; Krzyzanowski & Manson, 2022).

Various countries and regions have data protection laws impacting healthcare IT. For example, Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia has the Privacy Act, including the Australian Privacy Principles (APPs) that guide handling personal information, including health data.

Compliance with these regulatory frameworks is not just about legal obligation; it is critical to establishing trust between healthcare providers and patients. Ensuring data privacy in healthcare IT requires a comprehensive approach that includes technological solutions, employee training, and a culture of privacy and security within the organization (Bani Issa et al., 2020; Hathaliya & Tanwar, 2020). As technology evolves and the landscape of healthcare IT expands, ongoing efforts to address data privacy challenges and adapt to new regulations will be essential for protecting patient information and maintaining the integrity of the healthcare system.

4. Patient Consent in Healthcare IT

4.1. Concept and Importance of Consent

Informed consent is a foundational principle in both healthcare and research, rooted in the ethical obligation to respect patient autonomy and the right to self-determination. It requires that individuals are fully informed about and understand the nature of the medical treatment or research participation, including its risks, benefits, and alternatives, enabling them to make a voluntary and informed decision about their care or participation.

In healthcare IT, consent extends to how patient data is collected, used, stored, and shared. With the digitization of health records and the increasing use of digital platforms for patient care, ensuring informed consent for using personal health information has become more complex yet increasingly important. Consent in healthcare IT protects patient privacy and builds trust between patients and healthcare providers, ensuring that technology enhances patient care without compromising ethical standards (Jaiman & Urovi, 2020; Thapa & Camtepe, 2021).

4.2. Challenges in Obtaining Consent

Obtaining meaningful patient consent in healthcare IT presents several challenges. Firstly, there is the issue of comprehension. The technical nature of digital health services and data use policies can be daunting for patients to grasp. Medical jargon, complex terms of service, and the abstract nature of data processing can create a barrier, hindering patients' ability to fully understand what they are consenting to. Secondly, the voluntariness of consent can be compromised. Patients may feel that they have no choice but to consent to using their data, particularly when digital services are seamlessly integrated into their healthcare. This can lead to patients consenting not out of genuine agreement, but rather because they perceive it as necessary to receive the medical care they require.

Thirdly, the complexity of digital consent forms adds another layer of challenge. These processes are often lengthy and intricate, presented in formats that are not user-friendly. The overload of information and the impersonal nature of digital consent forms can further discourage patients from fully understanding or engaging with the information provided, potentially leading to uninformed consent. Lastly, the dynamic nature of digital health exacerbates the complexity of obtaining meaningful patient consent. Healthcare IT is constantly evolving, and the purposes for patient data use can change over time. This poses a significant challenge in ensuring that consent remains informed and reflective of future uses of data. In sum, addressing these challenges is crucial in safeguarding patients' rights and privacy in the ever-expanding realm of healthcare technology.

4.3. Strategies for Enhancing Consent Processes

Improving the consent process in healthcare IT requires thoughtful strategies that address its challenges while leveraging technology to facilitate better understanding and engagement. Consent materials should be clear, concise, and accessible. Using plain language, visual aids, and interactive tools can help demystify complex concepts related to data privacy and use.

Implementing a tiered consent model allows patients to choose different levels of data sharing according to their preferences. This approach respects patient autonomy by providing options rather than a single take-it-or-leave-it decision. Utilizing dynamic consent platforms that allow patients to modify their consent preferences over time can accommodate the evolving nature of healthcare IT and research (Haas et al., 2021). These platforms can provide ongoing communication and education, ensuring that consent remains informed. Providing educational resources and opportunities for patients to learn about the significance of their consent and the impact of digital health technologies on their care can empower patients to make more informed decisions.

Tailoring the consent process to patients' individual needs and preferences, including language preferences and accessibility needs, can enhance understanding and voluntariness. Engaging with patients to gather feedback on the consent process and making adjustments based on their experiences can improve the process and ensure it remains patient-centred (Bird et al., 2020). Healthcare IT can better align with ethical principles, protect patient rights, and foster a more trustworthy and patient-centered digital health ecosystem by addressing the challenges in obtaining patient consent and implementing strategies to enhance the consent process.

5. Ethical Issues in the Use of AI and Big Data in Healthcare

5.1. AI in Healthcare: Overview

Artificial Intelligence and big data in healthcare represent one of the most significant technological advancements in recent times, offering profound potential benefits for patient care, research, and healthcare management. Through machine learning and deep learning techniques, AI systems can analyze vast amounts of data to identify patterns, predict outcomes, and recommend treatments, often with accuracy and speed beyond human capability. Big data analytics in healthcare leverages large datasets from electronic health records (EHRs), genomic sequencing, wearables, and other sources to improve diagnostic processes, personalize medicine, and enhance public health surveillance (Rehman, Naz, & Razzak, 2022; Sauer et al., 2022).

The benefits of AI and big data in healthcare are substantial, revolutionizing the industry in several ways. Firstly, AI algorithms are pivotal in improving diagnostic accuracy, enabling faster and more precise disease diagnoses, such as cancer, which can significantly impact treatment outcomes. Moreover, big data analytics empowers healthcare providers to personalize treatments based on individual patient characteristics, enhancing the effectiveness of interventions. Additionally, AI aids in optimizing healthcare operations by streamlining hospital processes, reducing costs, and efficiently managing resources, ultimately improving the overall quality of patient care. Furthermore, AI accelerates drug development by expediting the discovery of potential therapies, shortening research timelines considerably compared to traditional methods (Niazi, 2023). Lastly, big data analytics improves public health by tracking disease outbreaks, informing evidence-based public health policies, and identifying population-level risk factors, all crucial for proactive disease prevention and management (Chao et al., 2023; Ibrahim & Saber, 2023).

5.2. Ethical Concerns

The integration of AI and big data in healthcare, while promising, introduces several ethical concerns that must be carefully navigated:

AI algorithms can perpetuate and even amplify biases in the data they are trained on. If historical data reflects past inequalities or biases (e.g., racial, gender, socioeconomic), the AI system may make biased predictions. This can lead to unequal care quality and outcomes among different patient groups, undermining healthcare's fairness and justice principles. AI systems, especially those based on deep learning, are often criticized for their "black box" nature, where the decision-making process is not transparent. This lack of transparency can make it difficult for clinicians to understand how AI reaches its conclusions, complicating informed decision-making and undermining trust in AI-supported healthcare solutions (Kundi, El Morr, Gorman, & Dua, 2023; Lopez, 2021).

Determining accountability for errors or adverse outcomes involving AI is complex. Questions arise as to who is responsible - the developers of the AI, the healthcare providers using it, or the institutions implementing it. The opacity of AI systems complicates matters further, making it challenging to pinpoint the source of errors. The use of big data in healthcare raises significant privacy concerns. The collection, storage, and analysis of large datasets, often containing sensitive health information, increase the risk of privacy breaches and unauthorized access. Ensuring data is used ethically and securely, in line with patient consent and privacy laws, is paramount. Obtaining informed consent for using patient data in AI and big data analytics is challenging. Patients may not fully understand the implications of their data being used this way, and the evolving nature of AI research and applications can make it difficult to outline specific uses at the time of consent (Keshta & Odeh, 2021; Thapa & Camtepe, 2021).

Addressing these ethical concerns requires a multidisciplinary approach that includes ethical oversight, developing transparent and explainable AI systems, ongoing monitoring for biases, robust data protection measures, and clear legal and regulatory frameworks. Engaging with patients, healthcare professionals, ethicists, and the public in developing and implementing AI and big data solutions in healthcare is crucial to ensure that these technologies enhance healthcare ethically, equitably, and socially responsible.

6. Solutions and Best Practices

Addressing the ethical considerations in healthcare IT, particularly around data privacy and patient consent, requires a multifaceted approach that combines technological innovations with robust policy frameworks.

6.1. Technological Solutions

Blockchain Technology: Blockchain offers a decentralized and secure framework for managing health data. By creating an immutable ledger of transactions, blockchain can ensure the integrity and confidentiality of patient data, providing a transparent and tamper-proof record. It can also facilitate secure and selective sharing of health information between authorized parties, enhancing patient control over their data and supporting the principle of informed consent (Westphal & Seitz, 2021; Zaabar, Cheikhrouhou, Jamil, Ammi, & Abid, 2021).

Advanced Encryption: Implementing state-of-the-art encryption methods is critical for protecting data at rest, in use, and transit. Homomorphic encryption, for instance, allows for computations on encrypted data, enabling the analysis of sensitive health information without exposing the actual data. This technology can be crucial in preserving patient privacy while leveraging data for research and clinical decision support.

Differential Privacy: Differential privacy introduces randomness into the data or data analysis outcomes, making it difficult to identify individual participants in a dataset. This approach can be particularly useful in research and public health surveillance, allowing for the utilization of health data while minimizing risks to individual privacy.

Consent Management Platforms: Digital platforms that enable dynamic and granular consent can empower patients to have greater control over their health data. These platforms allow individuals to specify their consent preferences, including what data can be shared, with whom, and for what purposes. They also facilitate easy updates to consent choices, reflecting patient preferences or changes in circumstances (Jaiman & Urovi, 2020).

6.2. Policy Recommendations

Policies should clearly define the rights and obligations of all parties involved in healthcare IT, including patients, providers, and technology vendors. Regulations should cover data collection, storage, use, sharing, and destruction, ensuring they align with ethical considerations and patient rights. Policies should mandate the transparency of healthcare IT systems, particularly those involving AI, ensuring that algorithms and data usage practices are understandable to patients and healthcare professionals. Establishing clear lines of accountability for decisions made with the assistance of or by healthcare IT systems is also crucial.

Regulations should require that consent processes are compliant with legal standards and accessible and understandable to patients. This includes providing information in plain language, offering options for granular consent, and ensuring that consent is freely given and can be easily withdrawn. Policy frameworks should encourage the development and use of AI in healthcare that is ethical, fair, and free of biases. This could include guidelines for the ethical design and implementation of AI systems, regular audits for bias and accuracy, and mechanisms for redress if AI systems cause harm.

Developing and implementing policies should involve collaboration between government bodies, healthcare organizations, technology companies, patients, and privacy advocates. Stakeholder engagement ensures that diverse perspectives are considered and policies are well-informed and balanced. It is essential to invest in education and training for healthcare providers, patients, and policymakers on the ethical use of healthcare IT, data privacy, and patient consent. Raising awareness and understanding of these issues can help promote best practices and compliance with ethical and legal standards. By combining technological innovations with thoughtful policy recommendations, it is possible to address the complex challenges of data privacy and patient consent in healthcare IT. This approach protects patients' rights and privacy. It fosters trust in digital health technologies, facilitating their potential to improve healthcare outcomes and efficiency.

7. Conclusion

This paper has explored the multifaceted ethical considerations in healthcare IT, focusing on data privacy and patient consent issues. We discussed the significant advancements in healthcare IT, their implications for patient care, and the ethical challenges posed by these technologies. The importance of ethical theories and principles in guiding healthcare IT practices was underscored, highlighting autonomy, beneficence, non-maleficence, justice, and the balance between

utilitarian and deontological approaches. The challenges of ensuring data privacy in the face of technical vulnerabilities, data breaches, and unauthorized access were examined, as were the complexities of obtaining genuine patient consent in an increasingly digital healthcare landscape. The potential of technological solutions like blockchain, advanced encryption, and consent management platforms to address these issues was highlighted, alongside policy recommendations to foster an ethical, transparent, and accountable use of healthcare IT.

The landscape of healthcare IT is rapidly evolving, driven by advancements in AI, big data analytics, and other digital technologies. Future research should focus on developing more sophisticated ethical frameworks that can adapt to these advancements. This includes exploring the ethical implications of emerging technologies, such as genomics and personalized medicine, and their impact on privacy and consent. There is also a need for interdisciplinary research that combines insights from ethics, law, technology, and healthcare to address the complex challenges at the intersection of these fields. Additionally, engaging with patients and the public in developing and implementing healthcare IT solutions can ensure that these technologies align with societal values and patient needs.

Maintaining ethical standards in the rapidly evolving domain of healthcare IT is paramount. As technologies advance, our ethical frameworks, policies, and practices must evolve to protect patient rights, ensure privacy, and foster trust in the healthcare system. This requires a concerted effort from all stakeholders, including healthcare providers, technologists, policymakers, and patients. By prioritizing ethical considerations in the development and use of healthcare IT, we can harness the immense potential of these technologies to improve patient care and public health while upholding the fundamental values of autonomy, privacy, and justice.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ahmad, G. I., Singla, J., & Giri, K. J. (2021). Security and Privacy of E-health Data. *Multimedia Security: Algorithm Development, Analysis and Applications*, 199-214.

[2] Ahmed, S. M., & Rajput, A. (2020). Threats to patients' privacy in smart healthcare environment. In *Innovation in Health Informatics* (pp. 375-393): Elsevier.

[3] Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the Implications of Healthcare Data Breaches through Computational Technique. *Intelligent Automation & Soft Computing, 32*(3).

[4] Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International nursing review, 67*(2), 218-230.

[5] Bhate, C., Ho, C. H., & Brodell, R. T. (2020). Time to revisit the Health Insurance Portability and Accountability Act (HIPAA)? Accelerated telehealth adoption during the COVID-19 pandemic. *Journal of the American Academy of Dermatology, 83*(4), e313-e314.

[6] Bird, M., Ouellette, C., Whitmore, C., Li, L., Nair, K., McGillion, M. H., . . . Carroll, S. L. (2020). Preparing for patient partnership: a scoping review of patient partner engagement and evaluation in research. *Health Expectations, 23*(3), 523-539.

[7] Byskov, M. F. (2020). Utilitarianism and risk. *Journal of Risk Research, 23*(2), 259-270.

[8] Chao, K., Sarker, M. N. I., Ali, I., Firdaus, R. R., Azman, A., & Shaed, M. M. (2023). Big data-driven public health policy making: Potential for the healthcare industry. *Heliyon, 9*(9).

[9] Char, D. S., Abràmoff, M. D., & Feudtner, C. (2020). Identifying ethical considerations for machine learning healthcare applications. *The American Journal of Bioethics, 20*(11), 7-17.

[10] Chukwuneke, F. N., & Ezenwugo, A. C. (2022). Deontology vs. Utilitarianism: Understanding the Basis for the Moral Theories in Medicine. *International Journal of Medicine and Health Development, 27*(1), 19-23.

[11] Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications, 177*, 102936.

[12] Haas, M. A., Teare, H., Prictor, M., Ceregra, G., Vidgen, M. E., Bunker, D., . . . Boughtwood, T. (2021). 'CTRL': an online, Dynamic Consent and participant engagement platform working towards solving the complexities of consent in genomic research. *European Journal of Human Genetics, 29*(4), 687-698.

[13] Haque, A. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems, 39*(5), e12753.

[14] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications, 153*, 311-335.

[15] Ibrahim, M. S., & Saber, S. (2023). Machine Learning and Predictive Analytics: Advancing Disease Prevention in Healthcare. *Journal of Contemporary Healthcare Analytics, 7*(1), 53-71.

[16] Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based health data sharing platforms. *IEEE access, 8*, 143734-143745.

[17] Javaid, M., Haleem, A., Singh, R. P., Rab, S., Suman, R., & Khan, I. H. (2022). Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. *International Journal of Cognitive Computing in Engineering, 3*, 124-135.

[18] John, S., & Wu, J. (2022). "First, Do No Harm"? Non-Maleficence, Population Health, and the Ethics of Risk. *Social Theory and Practice, 48*(3), 525-551.

[19] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal, 22*(2), 177-183.

[20] Krzyzanowski, B., & Manson, S. M. (2022). Twenty years of the health insurance portability and accountability act safe harbor provision: unsolved challenges and ways forward. *JMIR Medical Informatics, 10*(8), e37756.

[21] Kundi, B., El Morr, C., Gorman, R., & Dua, E. (2023). Artificial Intelligence and Bias: A scoping review. *AI and Society*, 199-215.

[22] Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. *Update of Selected Articles (May 4, 2021)*.

[23] Lopez, P. (2021). Bias does not equal bias: A socio-technical typology of bias in data-based algorithmic systems. *Internet Policy Review, 10*(4), 1-29.

[24] Niazi, S. K. (2023). The coming of age of ai/ml in drug discovery, development, clinical testing, and manufacturing: The FDA perspectives. *Drug Design, Development and Therapy*, 2691-2725.

[25] Patel, N. (2020). Social engineering as an evolutionary threat to information security in healthcare organizations. *Jurnal Administrasi Kesehatan Indonesia Volume, 8*(1).

[26] Pozgar, G. D. (2023). *Legal and ethical issues for health professionals*: Jones & Bartlett Learning.

[27] Rawling, P. (2023). *Deontology*: Cambridge University Press.

[28] Rehman, A., Naz, S., & Razzak, I. (2022). Leveraging big data analytics in healthcare enhancement: trends, challenges and opportunities. *Multimedia Systems, 28*(4), 1339-1371.

[29] Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation? *American Journal of International Law, 114*, 5-9.

[30] Safdar, N. M., Banja, J. D., & Meltzer, C. C. (2020). Ethical considerations in artificial intelligence. *European journal of radiology, 122*, 108768.

[31] Sauer, C. M., Chen, L.-C., Hyland, S. L., Girbes, A., Elbers, P., & Celi, L. A. (2022). Leveraging electronic health records for data science: common pitfalls and how to avoid them. *The Lancet Digital Health, 4*(12), e893-e898.

[32] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). *Healthcare data breaches: insights and implications.* Paper presented at the Healthcare.

[33] Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems, 91*, 101469.

[34] Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine, 129*, 104130.

[35] Varkey, B. (2021). Principles of clinical ethics and their application to practice. *Medical Principles and Practice, 30*(1), 17-28.

[36] Westphal, E., & Seitz, H. (2021). Digital and decentralized management of patient data in healthcare using blockchain implementations. *Frontiers in Blockchain, 4*, 732112.

[37] Wilkenfeld, D. A., & McCarthy, A. M. (2020). Ethical concerns with applied behavior analysis for autism spectrum" disorder". *Kennedy Institute of Ethics Journal, 30*(1), 31-69.

[38] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks, 200*, 108500.

[39] Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., . . . Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters, 8*(3), 66-77.