‘We may still not be ready for newer healthcare technologies’: An ethical perspective of privacy concerns

Appiah David [1] Majeed Duut Jamal-Deen [2]

Abstract

As healthcare technologies rapidly progress, a paramount concern arises: are individuals adequately prepared for the current challenges accompanying these advancements? Despite regulatory measures in place, the persistent issue of privacy demands heightened attention and prioritization. This essay aims to consistently underscore the significance of privacy in the evolving landscape of healthcare technologies, fostering a future where the advantages of these innovations are managed with responsibility. We present an ethical analysis addressing privacy apprehensions in emerging healthcare technologies, accompanied by recommendations for viable solutions to address these pressing concerns. It is concluded that hasty acceptance of new healthcare technology should be resisted, advocating instead for the allocation of resources and time to address privacy issues associated with emerging healthcare innovations. This commitment is indispensable for the well-being of patients, healthcare providers, technology enterprises, policymakers, activists, and the public.

Keywords

Artificial Intelligence (AI), Blockchain, Privacy and confidentiality, Healthcare technologies, Innovations

Authors
Appiah David [1] Department of Population Family and Reproductive Health, School of Public Health, University of Ghana, Accra-Ghana. Email: dappiah054@st.ug.edu.gh . ORCID ID: https://orcid.org/0000-0002-3810-4927

Majeed Duut Jamal-Deen [2] Department of Population Family and Reproductive Health, School of Public Health, University of Ghana, Accra, Ghana. Email: jmduut001@st.ug.edu.gh ORCID ID: https://orcid.org/0009-0007-4897-9253

Affiliations
Department of Population Family and Reproductive Health School of Public Health, University of Ghana, Accra, Ghana

Correspondence: Appiah David, davidappiah054@st.ug.edu.gh

Background

In the dynamic and swiftly changing realm of healthcare today, the incorporation of technology has brought about a revolution in health care provision. Healthcare technologies have significantly altered the way medical professionals, patients, and healthcare systems function, encompassing diagnostic instruments, treatment approaches, data administration, and patient welfare [1][2].

'Newer technologies' is a term that can be used to describe more recent technologies. Nanotechnology/Nanomedicine, biotechnology, cloud computing, internet of medical things (IOMTs), augmented reality, Radio Frequency Identification (RFID), voice search, chatbots, social media, blockchain, personalised medicine, biometrics, electronic health records, wearable computing, drones, robotics, and artificial intelligence are some of the technologies used in the healthcare industry [3].

Artificial Intelligence (AI) has been used for patient disease diagnosis, treatment, and monitoring, reducing human error, and improving decision support systems [3]. 3D printing offers precision solutions in various industries, including tissue and organ fabrication, prosthetics, implants, drug delivery, and clinical practice [4]. Virtual reality (VR) aids medical procedures, billing, and rehabilitation, reducing anxiety and offering the therapeutic potential for acute pain and anxiety disorders [5]. Nanomedicine, a combination of nanotechnology and medicine, revolutionizes disease diagnosis, management, and treatment, particularly in cancer treatment [6]. Robotics is increasingly integrated into healthcare delivery tools to address issues in surgery, diagnostics, prosthetics, therapy, monitoring, and support [7]. Cloud computing offers on-demand, self-service internet infrastructure for large scalable computing, storage, and data sharing, changing healthcare providers' services and addressing business and patient needs [8]. The Internet of Things (IoT) is being rapidly adopted for remote monitoring, smart sensor integration, and medical instrument integration [9]. Blockchain technology aids in accurate diagnoses and treatment prescriptions, providing one-stop access to patients' medical histories across providers [10].

One industry where IoT and AI, individually or together, are making significant impacts is the healthcare industry, which is constantly under pressure to reduce costs while addressing a rapidly growing unhealthy population [11]. Researchers also predicted an increase in the adoption of end-user wearable devices, with a total value of GBP 32.9 million in 2019. The advent of IoT-based Smart Healthcare systems in recent years has had a significant impact on the increasing demand for wearable electronics [12]. In 2020, the global IoT market generated an estimated 1.9 trillion dollars in economic value, primarily in the healthcare provider business [13]. Also, the European market for VR in healthcare is expected to reach $1.4 billion by 2025, with applications in pain management, rehabilitation, and surgical training [14].

As these healthcare innovations continue to advance, a growing concern emerges - are people truly prepared for the ethical implications and societal consequences of these newer technologies in healthcare? [15]. One major issue worth emphasizing is the privacy of patients' information [16].

Concern over the privacy and confidentiality of patient data is rising as electronic health records become more widely used and technology is incorporated into healthcare systems on a larger scale [17]. Issues of dependability, security, and privacy are particularly important because healthcare information is sensitive and there is a lot of reliance on reliable records [18]. Privacy and confidentiality are essential since sharing and digitizing health-related data could result in various sorts of attacks [19]. To provide a prominent level of security and privacy, numerous governmental health organizations have devised frameworks. For instance, the US Congress proposed the Health Insurance Portability and Accountability [19].

While the need to combine usability and effectiveness with privacy and security in innovation is well acknowledged, the truth is that technology is developing quickly, outpacing the creation and adoption of efficient security measures [20]. The frequency of data breaches in the healthcare sector has increased since 2010, and it is now one of the industry's most frequently attacked by cyberattacks globally, according to 2016 research by IBM and the Ponemon Institute [21]. Also, the use of technology in the healthcare industry raises the risk of revealing private health information, making it one of the top three industries with the highest yearly breach event rate [17]. Public Key Encryption (PKE) is frequently used to address a variety of security needs, including those for anonymity, collusion, etc. The capabilities and efficiency of PKE, however, need to be improved and enhanced given the widespread and comprehensive deployment of PKE infrastructure [19].

Two notable real-world examples illustrate the catastrophes and ethical challenges associated with healthcare technologies. First, the 2017 WannaCry ransomware attack on the National Health Service (NHS) in the United Kingdom compromised patient data and disrupted healthcare services, raising critical questions about data security and privacy in healthcare [22]. Second, studies have revealed that AI algorithms used for medical diagnosis may exhibit bias, leading to disparities in treatment recommendations for different demographic groups [23][24] .These instances raise ethical concerns surrounding fairness and equity in healthcare.

The ethical implementation of technology in healthcare is the deficit in current knowledge concerning the relationship between care-ethics and the efficiency of technology-mediated healthcare [25]. The lack of a proper ethical and legal framework surrounding the use of these recent technologies has led to extreme caution in their adoption and use by healthcare practitioners [26].

Efforts have been made to address these problems. Regulatory bodies have introduced guidelines and standards for data security and privacy in healthcare, and research is ongoing to reduce bias in AI algorithms [27]. However, the effectiveness of these measures remains a subject of scrutiny.

To move forward successfully with the implementation of modern technology, it is crucial to consider the challenges and concerns raised by healthcare professionals. As Sarewitz points out - the social, moral, and ethical implications of deploying modern technologies are contentious [28]. The emphasis should not be primarily on scientific discoveries or improvements alone, but rather on the potential negative consequences of these advancements.

This paper aims to provide an ethical analysis of data security and privacy concerns while offering recommendations to address this pressing issue. The goal of this paper is to maintain a constant focus on privacy as healthcare technologies continue to advance, thereby promoting a future where the benefits of these innovations are managed responsibly.

Ethical Analysis of Privacy Issues in Healthcare Technologies

Privacy Problem

In focus of this paper, privacy is explained in the dimension of information and decisional privacy. The informational dimension of privacy refers to the ability to regulate what other people know about oneself while decisional privacy refers to our control over our personal decisional sphere, aimed at protecting us from unwanted interference in our decisions and actions [23].

Many people's lives have been improved by technology since its early existence. It is undeniable that computers employed in healthcare have helped not only in terms of storing accurate and reliable patient information but have also improved the overall

operation of the healthcare industry. However, some social standards may not allow for the unrestricted sharing of personal information. It is well known that releasing one's personal information not only results in the disclosure of an entity's identity but also involves other significant people who may not have been notified, such as family members or community members [24].

Traditionally, in a healthcare facility, patients value the confidentiality of their personal health matters, while healthcare professionals prioritise the fulfilment of their professional responsibilities. Patients feel comfortable sharing health-related concerns in private rooms, ensuring privacy from other patients. This openness is motivated by the need for quality healthcare. Conversely, healthcare professionals maintain a boundary, disclosing only their name and professional role. This dynamic presents the asymmetry of vulnerability in private healthcare conversations, where patients reveal comprehensive personal details, and healthcare providers maintain a professional distance.

Karunarathne, et al. explained three types of healthcare-sensitive data: explicit identifiers, quasi-identifiers, and privacy attributes. In health records, explicit identifiers are personally identifiable information, whereas quasi-identifiers are unique personal information [25]. Specific identifiable information about a person is referred to as privacy attributes. These difficulties are addressed using random perturbation and data anonymization methods. Traditional anonymity, on the other hand, can result in privacy leaks [25]. Meanwhile, patients strongly prefer keeping their personal and health information confidential [26][27], and the idea of their private matters becoming a topic of conversation or being publicised makes them uncomfortable and unhappy.

Digital assistants such as Siri, Google assistant, Alexa among others created by prominent online platforms have the capacity to influence our decisions, inclinations, and actions, often prioritising the agenda of their creators or third parties over our individual interests[28]. The Internet of medical things and AI applied in telemedicine and mHealth functions invariably the same way. IoT features have inherent data privacy and security issues, including impersonation/identity spoofing, eavesdropping, data tampering, authorization, and control access issues, compromising and malicious code, availability and denial-of-service issues and cyberattacks [29]. Additionally, IoT devices, particularly those with advanced features like biometric sensors and health monitoring capabilities, pose significant privacy concerns due to their data collection and sharing mechanisms. Moreover, privacy concerns emerge [30]. Privacy and security concerns surrounding the use of technology in healthcare relate to data transfer and the recording of data transactions[31][32]. To illustrate, concerns regarding privacy and security were primarily viewed as obstacles to the acceptance of mHealth [33].

It is ethically relevant to examine privacy issues in newer healthcare technologies and prescribe solutions due to the profound consequences that may follow information and decisional breaches such that personal health information that has been accessed or disclosed without authorization may lead to feelings of vulnerability, anxiety, and a loss of trust in the healthcare system [34]. If sensitive health information is exposed, patients may face stigmatisation or discrimination based on their health conditions. This can affect their relationships, employment opportunities, and social interactions [34]. Identity theft or fraud resulting from a privacy breach can have financial consequences for the patient [35]. Stolen personal information may be used to commit fraudulent activities, such as obtaining medical services or prescriptions under the patient's name[36]. Also, as healthcare data becomes valuable for research and development, there is a risk of commercial entities exploiting patient data without proper consent [37].

Utilitarian perspective of Data privacy

Jeremy Bentham's utilitarianism theory, which deems actions ethically right if they contribute to the maximum happiness for the greatest number of people, supports the notion that respecting individuals' desire for privacy is morally imperative [38]. Since people want their matters to remain private, patients similarly wish to avoid the open publication and usage of their health information, as it could jeopardise their comfort and overall satisfaction.

The relationship between privacy and health technologies can be examined using a simplified hedonic calculation [39]. We can establish that in today's landscape, the proliferation of the Internet of Medical Things (IoMT), Artificial Intelligence (AI) in healthcare, mobile health (mHealth), and applications like wearables and virtual reality introduces a significant peril to patients' privacy.

Primarily, connected medical devices, such as smart insulin pumps and continuous glucose monitors in diabetes management, play a pivotal role in the IoMT. These devices actively generate and transmit real-time health data[40]. However, without robust security measures, unauthorised access to this data poses a grave threat to patient privacy. The potential consequences include unauthorised monitoring, misuse of health information, and a breach of confidentiality. Similarly, mobile health apps and wearable devices, like fitness trackers and heart rate monitors, amass diverse health-related data. In the absence of well-evaluated security measures, there is a risk of data interception during transmission or unauthorised access by third parties.

The repercussions of such privacy breaches extend beyond compromising personal health information. Patients may endure profound distress, facing potential social prejudice that could significantly impact their overall well-being. Moreover, unauthorised access to health records by malicious individuals, leading to potential harm or blackmail. These breaches not only imperil data security but also expose patients to significant emotional and physical risks.

In the domain of AI, which is increasingly prevalent in diagnostics and treatment planning, a potential risk arises when algorithms are trained on extensive datasets containing sensitive health information [41]. This raises the possibility of unintentional exposure of personally identifiable information. Additionally, concerning decisional privacy, patients may experience a loss of control over their decision-making sphere due to interference by AI algorithms through autosuggestions and decision-making processes. Consequently, patient autonomy in personal decisions may be influenced or compromised by the involvement of AI.

As hedonic calculation involves weighing the intensity, duration, certainty factors of pleasure and pain [42]. We can conclude that while improved healthcare services, research advancements, and convenience bring positive outcomes; privacy concerns, social stigma, and security risks contribute negative aspects.

Balancing technological innovations with privacy and promoting transparency align well with the core tenets of Utilitarian ethics. Therefore, to prioritise the overall happiness and well-being of individuals in the face of emerging healthcare technologies, there should be continuous evaluation and improvement of security measures in healthcare technologies. Also, transparency in AI algorithmic decision-making is crucial. However, it should not be seen as a substitute for ensuring that patients possess the essential information required to make decisions about the utilisation of their health data. In other words, while transparency in how algorithms operate is important, it does not replace the fundamental need for patients to be well-informed about how their health information is used and shared.

Privacy as a right

An individual's information goes beyond mere data; it unfolds as a narrative of their self and life. Consequently, this information is intrinsic to the individual, affording them the right to control who accesses it and how it is used. This right empowers the individual to exercise freedom in determining the handling of their personal information.

Wesley Hohfeld, the American legal theorist, identified four fundamental components of rights, known as "the Hohfeldian incidents." [43] These incidents have relevance in the context of modern technology, particularly in addressing privacy concerns and the assertion of one is right to privacy. The Hohfeldian incidents provide a framework for understanding and navigating rights, especially as they pertain to the evolving challenges posed by innovative technologies in healthcare. Indeed, the Hohfeldian incidents consist of privileges, claims, powers, and immunities. Privilege-rights delineate what their holder has no obligation to refrain from doing. For example, in the realm of privacy, a patient can disclose their health complaints only if they are not under any obligation to keep such information confidential. Therefore, the patient in question has the privilege to share health complaints to anyone.

The second Hohfeldian incident is claim-rights, where every claim-right corresponds to a duty in (at least) one duty-bearer. The duty-bearer's obligation is owed to the right-holder. Applying this concept to the context of healthcare, the patient is the right-holder, and the healthcare provider is the duty-bearer. Therefore, we logically assert, based on the claim-right incident, that a patient has a legitimate claim for their physician to keep information from their conversation confidential only if the physician has a duty to the patient to maintain the confidentiality of all interactions between them.

The third incident pertains to power in the Hohfeldian framework, allowing agents to modify claim-rights and privilege-rights. A patient possesses power if and only if they could alter their own or another person's Hohfeldian incidents. In the context of privacy, this implies that a patient can waive their claim to keep health information private by issuing an order, promise, or consent to share the information, thereby granting the recipient a corresponding privilege.

The fourth and final Hohfeldian incident is immunity. In the healthcare context, if a healthcare provider possesses the capability to modify a patient's claim-right or privilege claims, they have a power. In contrast, if a healthcare provider lacks the ability to alter the patient's Hohfeldian incidents, the patient has an immunity. This implies that, within the healthcare setting, the immunity incident ensures that the patient is shielded from the healthcare provider's capacity to share their information unless explicitly granted the power to do so through the patient's consent.

With the advent of modern technologies in healthcare, there is an increased collection of extensive information from patients' medical records that the patients may have initially shared with their healthcare providers. In such scenarios, patients claim privacy for their information, while healthcare providers or the industry bear the duty to ensure the confidentiality of the patient's information unless the patient exercises their power to permit disclosure and usage through explicit consent or waives their privacy rights.

However, it is often observed that the power dynamic can be skewed, making patients less immune to the actions of the healthcare industry. This imbalance can result in the sharing of information with third-party technology companies, such as wearable smart bands and virtual reality devices connected to internet of Medical Things (IOMTs) and AI systems. These technologies may capture or listen to information from the patient without the patient's awareness. The most significant concern arises when broad consents are employed, which are not specific about the information being gathered unknowingly from the patient. This lack of specificity can lead to the creation of predictive analyses from these powerful healthcare technologies without the patient's explicit understanding or consent.

Therefore, transparency, informed permission, and patient empowerment must be prioritised to resolve ethical problems raised by a lack of power-rights and unlawful data gathering in healthcare technologies. Healthcare practitioners and technology businesses should communicate clearly with patients about the capabilities and functionalities of the technologies that are being used. This includes specifying what data will be collected, how it will be used, and whether it will be shared with third-party groups and how they will prevent unauthorised access to their data. Also, it is critical to implement robust informed consent processes that fully specify the types of data that may be gathered, including any potential audio or visual information. It is critical to provide clear explanations regarding the aim of data gathering and how it contributes to patient care or research thus, providing granular consent options allows patients to decide the types of data they are comfortable sharing, ensuring they have control over their information and are fully aware of their consent decisions **Error! Reference source not found.**.

Virtues of Data privacy

Christine Swanton's advancements in target-centred virtue ethics [44] prove universally applicable when addressing privacy concerns in emerging healthcare technologies. Unlike the traditional focus on a virtuous individual, Swanton's approach centres on a healthcare industry striving to achieve virtuous targets in its practices. Therefore, target-centred virtue ethics departs from the eudemonistic assumption that virtues inherently benefit their possessor, offering a distinct perspective on evaluating ethical actions within the healthcare sector.

Target-centred virtue ethics is a variant of virtue ethics that assesses the morality of actions, emotions, and character traits based on the objectives or targets associated with virtuous qualities.
In the context of addressing privacy concerns in newer healthcare technology, these targets represent the ultimate ends or goals that virtues such as respect, reticence, and responsibility aim to achieve.

Respect

Respect is the virtue of treating patients as ends in themselves, not as means to our own ends. Respect for privacy means recognizing the dignity and autonomy of each patient the healthcare provider cares for, and not violating their medical confidentiality or preferences without their consent. In the same vein, respect for privacy also implies not exposing or compromising the identity or integrity of patients for the sake of others.

In the healthcare setting, virtuous targets are achieved and become evident as providers, administrators, and clinical researchers prioritise the utmost respect for patient information, recognizing it as integral and tangible to the well-being of the individual. The ethical treatment of data extracted from patient records must be carefully considered when using AI algorithms for diagnostic purposes and integrating the Internet of Medical Things (IoMT).

Patient data must be kept on a highly secure, classified media that is unaffected by hacking attempts from outside parties. It should be impossible to compromise on this security when it comes to technology and healthcare. Should information sharing be considered, the patient should be informed in advance and given clear explanations for its use. Crucially, getting the patient's consent ought to be an independent choice made without outside pressure.

Reticence

Reticence, the virtue of exercising restraint and discretion when disclosing or requesting information about others, is particularly relevant in the context of privacy. In terms of privacy, reticence entails refraining from revealing or requesting more information than is necessary or socially acceptable. It also involves being cognizant of the context and implications associated with sharing or collecting personal data.

Beyond simply avoiding the dissemination or misuse of information for malicious purposes, another dimension of privacy reticence involves using discretion in selecting both the sources and recipients of information. Achieving the target of reticence in managing patient records is vital for healthcare organisations. Upholding values that prioritise reticence not only sets a virtuous standard but also influences others within the organisation to meet these targets. This, in turn, fosters trust among patients and promotes a healthy environment for obtaining informed consent.

It is imperative for healthcare providers and support staff to exercise restraint in both intentional and unintentional disclosures, avoiding any loopholes that could potentially expose patient information to exploitation by unauthorised parties. In the current technological age, where complex and smart gadgets are utilised for health monitoring and information storage, there is a need for a robust link between the user and the information. This link should be secure and unbreachable while leveraging sophisticated security technologies that mandate multiple authentication steps before granting access. Examples include using an iris scanner, deep facial scanners, and other personalised methods to authenticate access to patient information [45], thereby ensuring the utmost privacy and security.

Responsibility

Responsibility, as a virtue, embodies accountability and reliability in one's actions and decisions. In the context of privacy, being responsible means recognizing and understanding the rights and obligations associated with the possession or processing of personal information and refraining from abusing or neglecting them. Additionally, responsibility for privacy involves taking a proactive and vigilant stance in safeguarding the privacy of others. It requires avoiding complacency or indifference to the potential risks and harms that may result from data breaches or misuse.

When the healthcare and IT industry actively commits to being responsible for securing patient information through the implementation of the latest innovations, it not only aligns with virtuous principles but also establishes trustworthiness within healthcare systems. This commitment contributes to improved health outcomes, as patients are more likely to trust and engage with systems that prioritise responsible handling of their sensitive information.

Counterargument from Communitarian ideals

Amitai Etzioni, Michael Sandel, and Charles Taylor have significantly influenced Communitarianism, an ideal that underscores the crucial role of community in shaping the social and political lives of individuals [46]. This perspective stands in opposition to theoretical liberalism, critiquing the over reliance on individual values like rights, freedom, and autonomy. Communitarianism strives to foster solidarity, unity, and the prioritisation of community values. Archbishop Desmond Tutu introduced a robust form of African Communitarianism, encapsulated in the popular saying "I am because we are," emphasising the importance of shared bonds over individual opinions [47].

In the realm of data privacy, moral rights and utilitarianism have often been used to support data privatisation. However, these viewpoints may clash with Communitarian ethics, particularly non-liberal Communitarianism [48]. According to Communitarianism, information about oneself is considered community property. In this context, the right to privacy of sensitive health information is not absolute. If revealing such information is deemed necessary for public safety or the well-being of the community, Communitarian's argue that it should be disclosed.

For example, a Communitarian perspective suggests that if an individual has diabetes and seeks treatment, their health record may be accessible to family, friends, and the community at large. This communal sharing of information is seen as essential for contributing to the person's healthcare and educating others in the community to promote preventive health. Communitarian's view utility differently, aligning it with actions that maximise community well-being, providing another approach to utilitarianism. Communitarianism emphasises the interconnectedness of individuals within a community, challenging traditional notions of privacy in favour of communal well-being.

In the realm of Artificial Intelligence (AI), the Internet of Medical Things (IoMT), and mobile health (m-health), a fresh perspective inspired by communitarian ideals advocates for the integration of privacy measures that extend beyond the individual patient. This approach emphasises the inclusion of significant others, such as family members, in the health information loop of patients utilising these technologies. According to this communitarian ideal, both the user (patient) and their family should have access to the health information of the family member, fostering a collaborative effort to support the overall well-being of the patient.

This shift towards inclusivity and shared health information promotes solidarity within health systems. It calls for interconnectedness and openness in the implementation of newer technologies, recognizing the importance of involving the patient's immediate community in the healthcare process. By prioritising the accessibility of health information to both the individual and their family, this approach aims to strengthen the support system around the patient, contributing to a more holistic and collaborative approach to healthcare in the age of advanced technologies.

Communitarianism offers an alternative viewpoint to our earlier discussions of the moral right to privacy as means of guaranteeing data privacy, particularly considering developing technological developments in medicine. Given the existence of these moral opposites, a critical analysis of justification and balance is necessary.

The Balance of Moral right and Communitarianism

Privacy as right and Communitarian ideals often stand in tension due to their differing perspectives on the individual's control over personal information and the role of the community in shaping social and political lives.

Privacy as a Right emphasises individual autonomy and the right to control one's personal information. Individuals have the authority to decide who accesses their data and how it is used, asserting that personal information is intrinsic to the individual, and they should have the freedom to determine its handling. However, Communitarian Ideals propose that certain information may be considered community property, especially in healthcare contexts. This perspective suggests that communal sharing of health information is necessary for public safety or the well-being of the community, challenging the absolute nature of individual privacy rights.

We understand how critical it is to strike a balance between individual privacy rights and communal objectives. While individual autonomy is important, certain situations may need restricted disclosure for the greater good of the society. As a result, specific criteria for exchanging health information in a way that respects individual rights while meeting societal requirements must be

established. When an individual's health threatens the lives of people in a community, health information may be shared at a communal level. However, to protect impacted persons from social harm associated with privacy breaches, this sharing should comply with anonymization methods. Furthermore, the exchange of health information should be limited in time and terminated once the public health emergency is determined to be under control.

Conclusion

We analysed privacy challenges in healthcare technologies, focusing on ethical principles that protect privacy. Notable challenges include concerns with online storage, access, and sharing of health records, data transfer risks, insufficient oversight for third-party developers, and contracts that fall outside of regulatory areas. As a result, any rush to accept new healthcare technology should be resisted, and a call is issued to devote funds and time in addressing privacy concerns related with emerging healthcare innovations. At the same time, the legal and regulatory framework surrounding healthcare technology should be strengthened to address privacy concerns associated with emerging technologies by pushing for universally acceptable privacy policies subjected to regular reviews. This involves preventing substandard devices from operating in the healthcare sectors worldwide, encouraging whistleblowing, and implementing stringent measures to ensure the safety to protect patient trust, especially as smart healthcare technologies are introduced. Moreover, healthcare innovators are urged to prioritise privacy factors to ensure a responsible and ethical advancement in the sector. This commitment is critical for the benefit of patients, healthcare providers, technology businesses, and the public.

Acknowledgements: The authors extend their gratitude to Mr. Christian Auagah and Ms. Comfort Adu Gyebi for their support.

Conflicts of Interest: None to declare

Authors' contributions
DA & JDM researched and wrote the manuscript. The authors read and approved the final manuscript.

Funding This work was not funded

Availability of data and materials
Not applicable.

Declarations
Ethics approval and consent to participate
Not applicable.
Consent for publication
Not applicable

References

[1] Mansour M. Letter from the Editor-in-Chief. The Journal of innovations in cardiac rhythm management. 2017 Jun 19;8(5): A7–7.
[2] Pawar A, Mary S. Artificial Intelligence in Medicine, and Healthcare. International Research Journal of Engineering and Technology [Internet]. 2020 Jun;7(6):5571–6. Available from: https://www.irjet.net/archives/V7/i6/IRJET-V7I61046.pdf
[3] Sadiku, NOM, Fagbohungbe OI, Musa SM. Artificial Intelligence in Healthcare: An Overview. International Journal of Engineering Research and Advanced Technology. 2020;06(12):38–45. Available from: https://doi.org/10.31695/IJERAT.2020.3670
[4] Trenfield SJ, Madla CM, Basit AW, Gaisford S. The Shape of Things to Come: Emerging Applications of 3D Printing in Healthcare. 3D Printing of Pharmaceuticals. 2018;1–19.
[5] Onyesolu MO, Eze FU. Understanding Virtual Reality Technology: Advances and Applications [Internet]. www.intechopen.com. IntechOpen; 2011 [cited 2024 Feb 11]. Available from: https://www.intechopen.com/chapters/14397
[6] Wong KK, Liu XL. Nanomedicine: a primer for surgeons. 2012 Aug 15;28(10):943–51. Available from: https://link.springer.com/article/10.1007/s00383-012-3162-y
[7] Kyrarini M, Lygerakis F, Rajavenkatanarayanan A, Sevastopoulos C, Nambiappan HR, Chaitanya KK, et al. A Survey of Robots in Healthcare. Technologies [Internet]. 2021 Jan 18;9(1):8. Available from: https://www.mdpi.com/2227-7080/9/1/8
[8] Griebel L, Prokosch HU, Köpcke F, Toddenroth D, Christoph J, Leb I, et al. A scoping review of cloud computing in healthcare. BMC Medical Informatics and Decision Making. 2015 Mar 19;15(1).
[9] Haghi Kashani M, Madanipour M, Nikravan M, Asghari P, Mahdipour E. A systematic review of IoT in healthcare: Applications, techniques, and trends. Journal of Network and Computer Applications [Internet]. 2021 Oct 15;192(192):103164. Available from: https://www.sciencedirect.com/science/article/pii/S1084804521001764
[10] Rani NK, Pravallika K,Nadiya SK, Poojitha T, Greeshma K. Block chain technology in healthcare: challenges and opportunities. International Journal of Health Care and Biological Sciences [Internet]. 2022 Jul 11 [cited 2022 Sep 16];51–5. Available from: https://www.saap.org.in/journals/index.php/ijhcbs/article/view/334/350
[11] Shah R, Chircu A. IoT and AI in healthcare: A systematic literature review. Issues in Information Systems. 2018 Jul 1;19(3).
[12] Poongodi T, Krishnamurthi R, Indrakumari R, Suresh P, Balusamy B. Wearable devices and IoT. A handbook of Internet of Things in biomedical and cyber physical system. 2020:245-73.
[13] Choi M, Kim S. Examining the Intention to Use Infant Health Monitoring Devices in South Korea [Internet]. Calgary: International Telecommunications Society (ITS); 2017 [cited 2024 Feb 11]. Available from: https://www.econstor.eu/handle/10419/168480
[14] Munster G, Jakel T, Clinton D, Murphy E. Next mega tech theme is virtual reality. gene. 2015 Feb 4; 612:303-6452.
[15] Kendal E. Ethical, legal, and social implications of emerging technology (ELSIET) symposium. Journal of Bioethical Inquiry. 2022 Sep;19(3):363-70.
[16] Kamalov F, Pourghebleh B, Gheisari M, Liu Y, Moussa S. Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. Sustainability. 2023 Feb 10;15(4):3317.
[17] Seh AH, Al-Amri JF, Subahi AF, Agrawal A, Pathak N, Kumar R, Khan RA. An analysis of integrating machine learning in healthcare for ensuring confidentiality of the electronic records. Computer Modeling in Engineering & Sciences. 2022 Jan 1;130(3):1387-422.
[18] Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian informatics journal. 2017 Jul 1;18(2):113-22.
[19] Azeez NA, Van der Vyver C. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal. 2019 Jul 1;20(2):97-108.
[20] Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC medical informatics and decision making. 2019 Dec;19(1):1-1.
[21] Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making. 2020 Dec; 20:1-0.
[22] Millard WB. Where Bits and Bytes Meet Flesh and Blood. Annals of Emergency Medicine. 2017 Sep;70(3): A17–21.
[23] Roessler B. The value of privacy. Cambridge: Polity Press; 2005
[24] Gürses S, Troncoso C, Diaz C. Engineering privacy by design. Computers, Privacy & Data Protection. 2011 Jan 29;14(3):25.
[25] Karunarathne SM, Saxena N, Khan MK. Security, and privacy in IoT smart healthcare. IEEE Internet Computing. 2021 Jan 18;25(4):37-48.
[26] Omole MS, Olanrewaju SA, Babafemi MO, Yaya AK, Michael EA. Knowledge and attitude of patients towards privacy and confidentiality of

health information in Nigeria (A Case Study of Medical Outpatients of Lagos University Teaching Hospital). American Journal of Pediatric Medicine and Health Sciences (2993-2149). 2023 Nov 6;1(9):359-72.
[27] Wagner AL, Zhang F, Ryan KA, Xing E, Nong P, Kardia SL, Platt J. US residents' preferences for sharing of electronic health record and genetic information: a discrete choice experiment. Value in Health. 2023 Feb 1.
[28] Stucke M, Ezrachi A. How your digital helper may undermine your welfare, and our democracy. Berkeley Technology Law Journal. 2018 May 28;32(3).
[29] Adams M. Big Data and Individual Privacy in the Age of the Internet of Things. Technology Innovation Management Review. 2017 Apr 19;7(4):12–24.
[30] Eruchalu CN, Pichardo MS, Bharadwaj M, Rodriguez CB, Rodriguez JA, Bergmark RW, et al. The Expanding Digital Divide: Digital Health Access Inequities during the COVID-19 Pandemic in New York City. Journal of Urban Health. 2021 Jan 20;98(2). Available from: https://doi.org/10.1007/s11524-020-00508-9
[31] Gordon WJ, Catalini C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal [Internet]. 2018 Jun 30;16:224–30. Available from: https://www.sciencedirect.com/science/article/pii/S200103701830028X
[32] Dwivedi A, Srivastava G, Dhar S, Singh R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors. 2019 Jan 15;19(2):326.
[33] Gagnon MP, Ngangue P, Payne-Gagnon J, Desmartis M. mHealth adoption by healthcare professionals: a systematic review. Journal of the American Medical Informatics Association. 2015 Jun 15;23(1):212–20.
[34] Stangl AL, Earnshaw VA, Logie CH, van Brakel W, C. Simbayi L, Barré I, et al. The Health Stigma and Discrimination Framework: a global, crosscutting framework to inform research, intervention development, and policy on health-related stigmas. BMC Medicine [Internet]. 2019 Feb 15;17(1). Available from: https://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-019-1271-3
[35] Koyame-Marsh RO, Marsh JL. Data breaches and identity theft: Costs and responses. IOSR Journal of Economics and Finance (IOSR-JEF). 2014; 5:36-45.
[36] Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul 1; 113:48-52.
[37] Wigan MR, Clarke R. Big data's big unintended consequences. Computer. 2013 Jun 7;46(6):46-53.
[38] Das D. Utilitarianism and longing for happiness. PalArch's Journal of Archaeology of Egypt/Egyptology. 2020 Nov 2;17(6):13246-51.
[39] Liszka J. Why happiness is of marginal value in ethical decision-making. J. Value Inquiry. 2005; 39:325.
[40] Rodríguez-Rodríguez I, Campo-Valera M, Rodríguez JV. Forecasting glycaemia for type 1 diabetes mellitus patients by means of IoMT devices. Internet of Things. 2023 Dec 1; 24:100945.
[41] Panayides AS, Amini A, Filipovic ND, Sharma A, Tsaftaris SA, Young A, Foran D, Do N, Golemati S, Kurc T, Huang K. AI in medical imaging informatics: current challenges and future directions. IEEE journal of biomedical and health informatics. 2020 May 29;24(7):1837-57.
[42] McFadden D. The new science of pleasure: consumer choice behaviour and the measurement of well-being. Handbook of choice modelling. 2014 Aug 29; 2:7-48.
[43] Wenar L. The nature of rights. In Rights: Concepts and Contexts 2017 May 15 (pp. 213-242). Routledge.
[44] Swanton C. Target Centred Virtue Ethics. Oxford University Press; 2021 Apr 15.
[45] Wells A, Usman AB. Privacy and biometrics for smart healthcare systems: attacks, and techniques. Information Security Journal: A Global Perspective. 2023 Oct 1:1-25.
[46] Etzioni A. Communitarianism revisited. Journal of Political Ideologies. 2014 Sep 2;19(3):241-60.
[47] Andoh CT. African communitarian bioethics and the question of paternalism. British Journal of Education, Society and Behavioural Science. 2016;15(4):1-6.
[48] Bell D. Communitarianism [Internet]. Stanford Encyclopedia of Philosophy. 2020. Available from: https://plato.stanford.edu/entries/communitarianism/