MAINTAINING CONFIDENTIALITY IN THE HEALTH TECH SPACE: EXPLORING LEGAL AND ETHICAL IMPLICATIONS

Nachanuya Silas Abangu*

ABSTRACT

Confidentiality is a cornerstone of the healthcare industry, especially in the rapidly advancing health tech space. The interconnectedness of digital health systems and the increasing reliance on technology in patient care pose unique challenges to maintaining confidentiality. This study aims to explore the legal and ethical implications surrounding the maintenance of confidentiality in the health tech space in Nigeria. The study begins by providing an overview of health tech and its increasing integration into healthcare systems. It then delves into the significance of maintaining patient confidentiality and the potential consequences of failing to do so. Drawing on legal frameworks and ethical principles, the essay analyses the legal obligations and responsibilities of healthcare providers and health tech companies in safeguarding patient information. The study discusses the challenges that may arise in maintaining confidentiality in the health tech space, including issues related to data breaches, third-party access, and patient consent. It also examines the evolving landscape of privacy laws and regulations, such as the National Health Act, Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners) and the Nigeria Data Protection Act, and their impact on health tech practices. Ethical considerations and challenges related to maintaining confidentiality in health tech are discussed, including data breaches, consent, and the sharing of patient information. The study concludes by underscoring the importance of collaboration between healthcare providers, health tech companies, policymakers, and regulatory bodies in shaping effective strategies to address the evolving legal and ethical complexities in maintaining confidentiality in the health tech space.

Keywords: *Confidentiality, Health Tech, Healthcare, Patients, Privacy,*

1. INTRODUCTION

Advancements in technology have revolutionised the healthcare industry, enabling the integration of health tech solutions into patient care. These technologies offer substantial benefits, including improved diagnosis, treatment, and monitoring of health conditions. However, the rise of health tech also raises concerns about the privacy and confidentiality of patient information in an increasingly digitised healthcare environment. This study explores the legal and ethical implications surrounding the maintenance of confidentiality in the health tech space, shedding light on the challenges faced by healthcare providers and health tech companies.

Maintaining patient confidentiality is a fundamental aspect of healthcare practice as it ensures that sensitive medical information remains private and secure. Breaches of patient confidentiality not only compromise an individual's privacy but can also lead to reputational

damage for healthcare organisations and erode patient trust.[1] As such, legal frameworks and ethical principles play a crucial role in safeguarding patient confidentiality in the health tech space. From a legal perspective, healthcare providers have legal obligations to protect patient confidentiality. The confidentiality of a patient in Nigeria draws strength from Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended), the Nigeria Data Protection Act, and the National Health Act. These legal frameworks regulate the use, disclosure, and security of protected health information and require healthcare organisations and health tech companies to implement robust security measures to protect patient confidentiality.

However, despite these legal requirements, maintaining patient confidentiality in the health tech space presents significant challenges. Technological vulnerabilities, such as data breaches and unauthorised access, pose substantial risks to patient privacy. The interconnected nature of health tech systems also raises concerns about third-party access to patient data. Also, the collection and integration of data from diverse sources, such as wearables, electronic health records, and telemedicine platforms, further complicates the protection of patient confidentiality. From an ethical standpoint, the preservation of patient confidentiality aligns with the core principles of healthcare ethics, including respect for autonomy, beneficence, and non-maleficence. Moreover, safeguarding patient privacy also fosters trust between healthcare providers and patients, promoting open and honest communication crucial for effective healthcare delivery.[2]

2. CONCEPTUAL CLARIFICATIONS

2.1 Confidentiality

Confidentiality in health law encompasses the duty of healthcare providers, institutions, and other entities to maintain the privacy and confidentiality of patient data.[3] This obligation extends to all forms of patient information, including medical records, diagnoses, treatment plans, test results, and any other details related to a patient's health.[4] It refers to "the principle of keeping secure and secret from others, information given by or about an individual in the course of a professional relationship,"[5] and it is the right of every patient, even after death.

Patient confidentiality has its origin in the first code of medical ethics.[6] The Hippocratic Oath, for example, states that "all that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread

---

* Legal Practitioner and an Assistant Lecturer at the Faculty of Law Modibbo Adama University, Yola, Adamawa State. Email: nsabangu@gmail.com Phone Number: +2348030510561.Address: K 157, Jada Street, Karewa GRA, Jimeta, Yola, Adamawa State.

1 J.M. Jeffords, 'Confidentiality of Medical Information: Protecting Privacy in an Electronic Age' *Professional Psychology: Research and Practice* (1999) 30 (2), 115–116. <https://doi.org/10.1037/0735-7028.30.2.115> accessed 24 June 2024

2 T.L. Beauchamp & JF Childress, *Principles of Biomedical Ethics* (5th edn, Oxford University Press 2001)

3 N.S. Almaghrabi, and A.B. Bussma "Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature." *Dr. Sulaiman Al Habib Medical Journal* (2022) (4) (3) 126-135.

4 *Ibid*

5 J. Bourke and S. Wessely, 'Confidentiality' *BMJ.com* (2008) 336 <https://doi.org/10.1136/bmj.39521.357731.BE> accessed 25 June 24, 2024

6 E. Jackson, *Medical Law: Text, Cases and Materials* (5th edn, Oxford University Press 2019) 420

abroad, I will keep secret and will never reveal." Patient confidentiality also received unqualified protection from the modern version of the Oath, the Declaration of Geneva (as amended 1994), thus "I will respect the secrets which are confided in me even after the patient has died." Consequently, a doctor shall preserve absolute secrecy on all that he knows about his patient because of the confidence entrusted in him.[7]

Confidentiality of patients' information is a crucial aspect of maintaining privacy, trust, and respect in healthcare relationships. It ensures that patients can freely and openly communicate with healthcare providers while having confidence that their personal health information will be protected and used appropriately.

2.2 Health Technology (Health Tech)

Health tech, also known as digital health or healthcare technology, refers to the application of technology and digital solutions in the healthcare industry to improve patient care, enhance efficiency, and facilitate access to healthcare services.[8] It encompasses a wide range of technologies, including electronic health records (EHRs), telemedicine, wearable devices, mobile health applications, and artificial intelligence (AI) systems.[9] Health tech also refers to the use of technologies developed for the purpose of improving all aspects of the healthcare system. [10]

Health technology is defined as the application of organized knowledge and skills in the form of devices, medicines, vaccines, procedures and systems developed to solve a health problem and improve the quality of lives.[11] Similarly, the World Health Organisation (WHO) defines health technology as the application of organised knowledge and skills in the form of medicines, vaccines, medical devices, and procedures, alongside systems that are used to solve numerous health problems and improve the quality of life across the world.[12]

The integration of health tech in healthcare systems has the potential to transform healthcare delivery and improve patient outcomes. It offers opportunities for more accurate diagnoses, personalised treatment plans, remote patient monitoring, and improved communication between healthcare providers and patients. For instance, EHRs enable the electronic storage and exchange of patient health information, facilitating seamless communication between healthcare providers and improving care coordination.[13] Telemedicine allows remote access to healthcare services, particularly in underserved or rural areas, connecting patients with healthcare providers through video conferencing and remote

---

7 World Medical Association's International Code of Ethics (1949)

8 S. Agboola et al., 'Digital Health and Patient Safety' *JAMA* (2016) 315 <10.1001/jama.2016.2402> accessed 25 June 2024

9 R.L. Bashshur et al., 'The Empirical Foundations of Telemedicine Interventions in Primary Care' *Telemedicine journal and e-health* (2016) 22 (5) 342-75 < https://doi.org/10.1089/tmj.2016.0045> accessed 26 June 2024

10 S. Daley, *Healthcare Technology 101* (2022) <https://builtin.com/healthcare-technology> accessed 26 June 2024

11 M. Maschio and F. Paladin, *Epilepsy and Brain Tumor* (Academic Press 2015) 257-268.

12 World Health Organization, What Is Health Technology? <https://www.who.int/teams/health-product-policy-and-standards/assistive-and-medical-technology/medical-devices/assessmen> accessed 27 June 2024

13 N. Menachemi and T.H. Collum, 'Benefits and Drawbacks of Electronic Health Record Systems' *Risk Manag Healthc Policy* (2011) (4) 47-55 <https://doi.org/10.2147/RMHP.S12985> accessed 27 June 2024

monitoring.[14] Wearable devices, such as fitness trackers and smart watches, provide real-time health data, empowering individuals to monitor their health and engage actively in disease prevention and management.[15]

3. REGULATORY AND STATUTORY FRAMEWORK FOR CONFIDENTIALITY RIGHTS

The regulatory and statutory framework for confidentiality rights in health law primarily centres around the protection of patient privacy and the confidentiality of health information. In Nigeria, this right is protected by a combination of statutes, regulations, and professional codes of ethics. Below is an overview of the key elements of those statutes and regulations:

3.1 Constitution of the Federal Republic of Nigeria 1999 (As Amended)

Section 37 of the 1999 Constitution of Nigeria is a pivotal legal provision that addresses the right to privacy, which includes the confidentiality of personal information, such as medical records. This section provides, "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." This constitutional guarantee is significant for the healthcare sector, as it establishes a legal foundation for the confidentiality of patient medical records, thereby promoting trust between patients and healthcare providers. The section establishes a legal framework for privacy and reinforces the ethical obligations of healthcare practitioners, and provides a basis for legal recourse in cases of breaches.

The implications of Section 37 extend to various healthcare practices, particularly in ensuring that patient information is not disclosed without consent. This aligns with the ethical obligations of healthcare professionals to maintain confidentiality. This constitutional protection of privacy serves as a legal backing for healthcare practitioners, reinforcing their duty to protect sensitive patient information from unauthorised access or disclosure. The increasing use of electronic health records (EHRs) poses new challenges for maintaining confidentiality.[16] The transition to digital records necessitates robust security measures to protect patient information from breaches, which is a growing concern in Nigeria's healthcare system. The constitutional right to privacy, as enshrined in Section 37, also mandates that healthcare providers implement adequate safeguards to protect electronic medical records from unauthorised access, thereby ensuring compliance with both legal and ethical standards.

3.2 The National Health Act, 2014

Nigeria's National Health Act provides a legal framework for the regulation, development, and management of Nigeria's Health System. The Act recognises the importance of confidentiality. Section 26 (1) of the Act is clear on the confidentiality of patients; it provides thus: “All information concerning a user, including information relating to his or her health

---

[14] R.L. Bashshur et al., ‘The Empirical Foundations of Telemedicine Interventions in Primary Care’ *Telemedicine journal and e-health* (2016) 22 (5) 342-75. https://doi.org/10.1089/tmj.2016.0045 accessed 26 June 2024

[15] S.R. Steinhubl et al., "The Emerging Field of Mobile Health" *Science Translational Medicine* (2015) (7) 283 <https://doi.org/10.1126/scitranslmed.aaa3487> accessed 27 June 2024

[16] N.N. Basil, et al., ‘Health Records Database and Inherent Security Concerns: A Review of the Literature.’ *Cureus* (2022) *14* (10).

status, treatment or stay in a health establishment is confidential." This section emphasises the importance of safeguarding patients' personal and medical information from unauthorised access, use, and disclosure. Subsection 2 of Section 26 of the Act stipulates the circumstances where such confidential information can be disclosed, which include the patient's written consent and by an order of court. In a case where the patient is a minor, such disclosure will require the consent of a parent or guardian. In the case of a person who is otherwise unable to grant consent upon the request of a guardian or representative.[17] Section 27 of the Act provides the two legal basis when disclosure of health record of a user can be made available to a third party, another healthcare provider or professional, which include if the disclosure is necessary for any legitimate purpose within the ordinary course and scope of his or her duties; and when such access or disclosure is in the interest of the user. The latter is similar to using vital interest as the legal basis.

The National Health Act also made provisions for the Protection of Health records by succinctly stating: "the person in charge of a health establishment who is in possession of a user's health records shall set up control measures to prevent unauthorized access to those records and to the storage facility in which, or system by which, records are kept." Healthcare providers are required to maintain strict confidentiality and only access patient records for the purpose of providing care or treatment. Any breach of confidentiality is considered a violation of the law and may lead to legal sanctions. Section 28 (1) provides that a healthcare provider can access the health record of a patient with the consent of the patient. This provides for consent as a legal basis. The section also allows health records to be used for research with the consent of the patient. Section 28 (2) provides that the authorisation of the patient or any other authority can be dispensed with for the purposes of research, teaching and studying if the research data does not contain any personally identifiable information. Section 29 (2) (j) (ii) provides that "any person who without authority, modifies or impairs the operation of any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept, commits an offence and is liable on conviction to imprisonment for a period not exceeding two years or to a fine of N250,000.00 or both."

From the foregoing provisions, it is crucial for healthcare professionals to uphold the confidentiality of patient records to ensure trust and privacy in the healthcare system. The National Health Act did not only prioritised the confidentiality of a patient's health record but also went further to criminalise unauthorised use or access to such information, which signals the importance attached to confidentiality by the law.

3.3 The Nigeria Data Protection Act, 2023

The Act establishes the legal framework for the regulation of personal data in Nigeria and replaces the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019 issued under the National Information Technology Development Agency (NITDA) Act. The Act is designed to safeguard the privacy of individuals and regulate the processing of personal data by public and private entities. Its

[17] Section 26 (2) (b) (ii) National Health Act, 2014

implications for the confidentiality of patient medical records are profound, as it establishes clear guidelines and legal obligations for healthcare providers and institutions.

The Act empowers the Commission to superintend the implementation and enforcement of rules and regulations set out in the Act, and regulates the processing of personal information and other related matters. Some of the key objectives of the Act[18] is to regulate the processing of personal data, promote data processing best practices that safeguard the security of personal data and the privacy of data subjects, protect the rights of data subjects and providing means of recourse and remedies, in the event of the breach of the data subjects' rights and ensuring that data controllers/ processors fulfill their obligations to data subjects. The data sought to be protected by the Act includes the medical information of patients and individuals in Nigeria. The Act defines personal data[19] and emphasises the importance of consent[20] in the processing of such data. Specifically, it states that personal data must be processed lawfully, fairly, and transparently, with the explicit consent of the data subject.[21] This provision is crucial for patient confidentiality, as it mandates that healthcare providers obtain informed consent before disclosing or processing any medical records.

3.4 Freedom of Information Act

The Freedom of Information Act, enacted in 2011, is a significant piece of legislation aimed at promoting transparency and accountability in governance.[22] However, its implications for the confidentiality of patient medical records are complex and multifaceted. While the Act seeks to enhance public access to information held by public authorities, it also raises critical concerns regarding the protection of sensitive personal data, particularly in the healthcare sector.

Section 1 of the Act establishes the right of citizens to access information held by public institutions, which includes health records maintained by government hospitals and health agencies. However, this right is not absolute and is subject to certain exemptions, particularly concerning personal privacy. Section 14 of the Act explicitly states that information that would constitute an invasion of privacy is exempt from disclosure. This provision is crucial in safeguarding the confidentiality of patient medical records, as it recognises the need to protect sensitive health information from public exposure. Section 16 of the Act further provides that a public institution may deny an application for information that is subject to the health workers-client privilege. This section provides a legal backing for the professional confidentiality obligation of a health worker.

The Freedom of Information Act plays a dual role in the context of patient medical records. While it promotes transparency and accountability, it also recognises the importance of protecting individual privacy rights. Ensuring that patient information remains confidential while promoting access to information is essential for fostering trust in the healthcare system and encouraging individuals to seek necessary medical care.

---

18 Section 1 National Data Protection Act 2023
19 Section 65 National Data Protection Act 2023
20 Section 26 National Data Protection Act 2023
21 Section 24 National Data Protection Act 2023
22 C.W. Duru, 'The Relevance of Nigeria's Freedom of Information Act (2011) to the Country's Anti-corruption War.' *Journalism* (2016) *6*(12), 757-762.

3.5 Medical and Dental Practitioners Act

The Medical and Dental Practitioners Act in Nigeria is a crucial legislative framework that governs the practice of medicine and dentistry in the country. One of its significant aspects is the protection of patient confidentiality, which is essential for maintaining trust in the healthcare system. The Act emphasises the importance of safeguarding patient medical records, aligning with broader ethical and legal standards that govern medical practice.

The Medical and Dental Practitioners Act provides for the establishment of the Medical and Dental Council of Nigeria.[23] The Medical and Dental Council of Nigeria (MDCN) regulates the practice of medicine and dentistry in Nigeria, including setting professional standards and guidelines for healthcare professionals. These guidelines emphasise the importance of patient confidentiality and the ethical obligations of healthcare practitioners to maintain privacy and protect patient information.

3.6 Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners) 2004

The Rules of Professional Conduct for Medical and Dental Practitioners in Nigeria, established by the Medical and Dental Council of Nigeria (MDCN), provide a comprehensive framework that governs the ethical and professional behaviour of healthcare practitioners. One of the critical aspects of these rules is maintaining the confidentiality of patient medical records, which is fundamental to the trust-based relationship between patients and healthcare providers.

Rule 44 of the Code on Medical Ethics in Nigeria requires that "privileged information" divulged to the practitioner during treatment must not be revealed to a third party.[24] The Rule explicitly states that a practitioner must not disclose any information relating to a patient's medical condition or treatment without the patient's consent, except where required by law. This provision underscores the ethical obligation of healthcare providers to protect patient confidentiality and highlights the necessity of obtaining informed consent before disclosing any medical information. Furthermore, Rule 44 emphasises that practitioners must ensure that all staff members who have access to patient records are aware of the importance of confidentiality and are trained to handle such information appropriately. This provision is crucial in healthcare settings where multiple personnel may interact with patient records, as it helps to mitigate the risk of inadvertent breaches due to a lack of awareness or training.

The increasing use of electronic health records (EHRs) presents new challenges for maintaining confidentiality. The Rules of Professional Conduct require practitioners to implement adequate security measures to protect electronic records from unauthorised access.[25] This is particularly relevant in Nigeria, where the transition to digital health records is ongoing, and the risks associated with data breaches are significant. Healthcare institutions

---

23 Section 1 Medical and Dental Practitioners Act, 2004.

24 Rule 44 Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners) 2004.

25 Rule 22 Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners) 2004.

must ensure that they have robust data protection policies in place to comply with both ethical and legal standards.[26]

4. CONFIDENTIALITY IN THE HEALTH TECH SPACE

Confidentiality in the health tech space refers to the obligation to protect sensitive patient information, ensuring that it remains private and secure. It encompasses the safeguarding of personal health records, medical history, test results, and any other identifiable health data.[27] Maintaining confidentiality in the health tech space is critical for preserving patient trust, respecting individual autonomy, and protecting sensitive information from unauthorised access or disclosure. From a legal standpoint, healthcare providers and health tech companies have clear obligations to maintain patient confidentiality. Laws such as the Medical and Dental Practitioners Act, Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners), and National Health Act, among others, set guidelines for safeguarding patient data. These regulations establish the rights of patients when it comes to the use and disclosure of their health information, as well as the responsibilities of healthcare organisations in ensuring data privacy and security.

In addition to legal requirements, ethical considerations play a significant role in defining the nature of confidentiality in the health tech space. Ethical principles, such as respect for autonomy, beneficence, and non-maleficence, guide the responsible handling of patient data. Healthcare providers and health tech companies must prioritise patient privacy by obtaining informed consent before collecting, using, or sharing health information. It is crucial to ensure that individuals are fully aware of how their data will be utilised, the potential risks involved, and the steps taken to protect their privacy. Open and transparent communication between healthcare providers, health tech companies, and patients is fundamental in establishing trust, ensuring individuals have control over their personal health information, and fostering a patient-centric approach to data confidentiality.[28]

Technological advancements also influence the nature of confidentiality in the health tech space. The increasing use of electronic health records, telemedicine, wearable devices, and mobile apps presents both opportunities and challenges.[29] While these technologies facilitate data collection, analysis, and remote healthcare delivery, they also raise concerns regarding data security and privacy. To mitigate these risks, health tech companies must implement robust data security measures, which include encryption techniques, secure storage systems, access controls, and regular vulnerability assessments. Additionally, data

---

[26] M.Y. Ijadunola, 'Lifting the Veil on Disrespect and Abuse in Facility-Based Childbirth Care: Findings from South West Nigeria.' *BMC Pregnancy and Childbirth* (2019) <19(1).https://doi.org/10.1186/s12884-019-2188-8> accessed 14th November 2024.

[27] N.P. Terry et al., 'Ensuring the Privacy and Confidentiality of Electronic Health Records' *U. Ill. L. Rev.* (2007) 681. <http://hdl.handle.net/10822/967881> accessed 26 June 2024

[28] B.A. Nielsen, 'Confidentiality and Electronic Health Records: Keeping Up with Advances in Technology and Expectations for Access' *Clinical Practice in Pediatric Psychology* (2015) 3 (2), 175–178.

[29] J.R. Rodriguez-Feliz et al., 'The Mobile Technology Era: Potential Benefits and the Challenging Quest to Ensure Patient Privacy and Confidentiality' *Plastic and Reconstructive Surgery (Journal of the American Society of Plastic Surgeons* (2012) 130 (6) 1395-1397 <http://10.1097/PRS.0b013e31826d9d81> accessed 30 June 2024

anonymisation and de-identification techniques should be employed to protect the privacy of individuals, ensuring that patient data cannot be linked back to specific individuals.

4.2 Confidentiality Obligations and Responsibilities of Healthcare Providers and Health Tech Companies

The healthcare providers and health tech companies have the following confidentiality obligations and responsibilities towards patients:

1. *Maintaining Patient Data Privacy***:** Healthcare providers and health tech companies must ensure the security and privacy of all patient data, including medical records, diagnoses, treatments, and personal information.[30] This includes implementing robust data security measures, limiting access to authorised personnel, and adhering to data privacy regulations like the Nigerian Data Protection Act, Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners), National Health Act, among others.
2. *Obtaining Informed Consent***:** Before collecting or sharing any patient data, healthcare providers and health tech companies must obtain informed consent from the patient and explain to the patient how the data will be used, stored, and protected.[31] Such consent should be clear, specific, and voluntary.
3. *Implementing Strict Access Controls:* Health tech companies must enforce access controls to limit who can view and handle patient information.[32] Only authorised personnel should have access, and proper authentication and encryption methods should be employed.
4. *Addressing Security Breaches***:** Develop and implement clear protocols for responding to data breaches that minimise harm to patients.[33] This includes promptly notifying affected individuals, taking corrective action, and improving security measures to prevent future breaches.
5. *De-Identifying and Anonymising Data***:** To further protect patient privacy, healthcare providers and health tech companies should de-identify and anonymise patient data whenever possible, so that individuals cannot be identified based on their health information.[34]
6. *Implementing Secure Storage and Disposal Methods***:** Healthcare providers and health tech companies should employ secure storage and disposal methods for patient data. This should include regular updates and patches to protect against vulnerabilities and proper data sanitisation when deleting or disposing of data.[35]

---

30 R.A. Tariq and P.B. Hackert, *Patient Confidentiality* (Treasure Island (FL): StatPearls Publishing; 2023).

31 P. Shah et al., *Informed Consent* (Treasure Island (FL): StatPearls Publishing; 2023).

32 National Research Council (US) Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the Record Protecting Electronic Health Information. Washington (DC): National Academies Press (US); 1997. 4, Technical Approaches to Protecting Electronic Health Information. Available from: <https://www.ncbi.nlm.nih.gov/books/NBK233433/> accessed 4 July 2024

33 *Ibid*

34 C.A. Kushida et al., 'Strategies for De-Identification and Anonymization of Electronic Health Record Data for Use in Multicenter Research Studies' *Med Care* (2012) 82-101.

35 P. Sloan and D.H. Juhnke, 'Secure Disposal of Medical Practice Records' *Journal of the Missouri State Medical Association* (2016) 264-266.

7. *Training Employees on Confidentiality*: Healthcare providers and health tech companies should train their employees and staff on the importance of patient confidentiality, data protection protocols, and regulatory compliance.
8. *Complying with Legal and Regulatory Requirements*: Healthcare providers and health tech companies must adhere to applicable laws and regulations regarding patient confidentiality, such as the Medical and Dental Practitioners Act, Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners), National Health Act, among others.

4.3 Legal and Ethical Implications of Maintaining Confidentiality in The Health Tech Space

Maintaining confidentiality in the health tech space carries significant legal and ethical implications impacting both healthcare providers and health tech companies. Understanding these implications is crucial for ensuring compliance, avoiding penalties, and maintaining trust with patients. Some of the key issues are broadly considered below:

1. *Data Collection and Sharing*:
   a. Consent and Transparency:[36] How can informed consent be obtained from patients when their data is shared or aggregated with others, possibly for secondary purposes like research or commercial use?
   b. De-Identification and Anonymisation:[37] Can data truly be anonymised in a way that prevents re-identification, especially with the advancement of data analysis techniques?
   c. Control and Ownership: Who owns the rights to an individual's health data collected through health tech platforms, and how much control do patients have over its use and dissemination?

Striking a balance between utilising patient data for research and innovation purposes while ensuring that individual privacy is respected is fundamental. It is important to obtain informed consent from individuals before using their data, ensuring that they understand how their information may be utilised and the potential risks involved.

2. *Security and Breaches*:
   a. Vulnerability to Cyberattacks:[38] Health tech systems are prime targets for hackers, potentially exposing sensitive medical information. What measures can be taken to mitigate risks and prevent data breaches?
   b. Third-Party Involvement:[39] Many health tech platforms rely on third-party vendors for data storage and processing, leading to concerns about the security practices and oversight of these entities.

---

36 M.L. Eaton and D. Kennedy, *Innovation in medical technology: Ethical issues and challenges* (Johns Hopkins University Press: Baltimore 2007)

37 B. Kaplan, 'Selling Health Data: De-Identification, Privacy, and Speech' *Cambridge Quarterly Healthcare Ethics* (2015) 24 (3) 256-71.

38 E.H. Kluge, 'Ethical and Legal Challenges for Health Telematics in a Global World: Telehealth and the Technological Imperative' *Int J Med Inform* (2011) 80 (2) <https://doi.org/10.1016/j.ijmedinf.2010.10.002> accessed 25 July 2024

39 I.G. Cohen et al., 'The Legal and Ethical Concerns that Arise from Using Complex Predictive Analytics in Health Care.' *Health affairs* (2014) 1139-1147.

c. Transparency and Accountability[40]: How should data breaches be handled, and what procedures are in place to inform patients and hold parties accountable for security failures?

Protecting patient data from cyberattacks or breaches requires robust security measures and constant monitoring. Health tech companies must invest in up-to-date technologies and protocols to ensure data integrity and confidentiality.[41]

3. *Algorithmic Bias and Discrimination*:
   a. Fairness and Equity:[42] When health tech algorithms are used for decision-making (e.g., diagnosis, treatment recommendations), how can we ensure that they are free from bias that could disproportionately disadvantage certain groups?
   b. Explainability and Transparency: Can algorithms be designed to be transparent and explainable, allowing patients and healthcare professionals to understand how decisions are made based on their data?
   c. Mitigating Bias and Discrimination:[43] What strategies can be employed to identify and address potential biases in health tech algorithms to ensure fair and equitable healthcare outcomes for all?

Healthcare algorithms and Artificial Intelligence (AI) bias can contribute to existing health disparities for certain populations based on race, ethnicity, gender, age, or other demographic factors.[44] One reason for healthcare algorithm and AI bias is the lack of diversity in the data used to train computer programs. It is therefore important for the healthcare providers and health tech companies to ensure that the programs are trained on data to protect patient privacy and prevent potential discrimination or stigmatisation.

4. *Secondary Use of Data and Public Good:*
   a. Balancing individual privacy with public health benefits: Balancing patient privacy with the potential benefits of using health data for public health research, disease surveillance, or personalised medicine interventions poses a complex ethical dilemma.[45]
   b. Patient trust and engagement: How can we ensure that patients understand the potential benefits and risks of their data being used for secondary purposes, and encourage their trust and participation in such initiatives?

---

40 W.N. Price and I.G. Cohen, 'Privacy in the Age of Medical Big Data.' *Nature medicine* (2019) 25 (1) 37-43.

41 M. Javaid et al., 'Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends' *Cyber Security and Applications*, (2023) 1<https://doi.org/10.1016/j.csa.2023.100016.> accessed 26 July 2024

42 B. Stanberry, 'Legal and Ethical Aspects of Telemedicine.' *Journal of Telemedicine and Telecare* (2006) 12 (4) 166-175. <https://doi.org/10.1258/135763306777488825> accessed 25 July 2024

43 S. Hoffman and A. Podgurski, 'Artificial Intelligence and Discrimination in Health Care' *Yale Journal of Health Policy, Law, and Ethics* (2021) <http://hdl.handle.net/20.500.13051/5964> accessed 26 July 2024

44 L.H. Nazer et al., 'Bias in Artificial Intelligence Algorithms and Recommendations for Mitigation' *PLOS Digit Health* (2023) 2 (6) <https://doi.org/10.1371%2Fjournal.pdig.0000278> accessed 4 August 2024

45 J.G. Hodge Jr. et al., 'Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability'. *Jama* (1999) 282 (15) 1466-1471.

c. Regulatory frameworks and governance: Robust and transparent regulatory frameworks are needed to govern the secondary use of health data, ensuring informed consent, ethical standards, and accountability mechanisms.[46]

In maintaining confidentiality, health tech companies must also consider the potential risks of data sharing among third parties or collaboration with academic institutions. Proper agreements and protocols should be in place to ensure that data is used and shared responsibly and in accordance with relevant laws and regulations.

Addressing these legal and ethical dilemmas requires a multi-pronged approach. It involves developing clear ethical guidelines, implementing robust data security measures, ensuring transparency and accountability throughout the healthcare data ecosystem, promoting patient education and empowerment, and continuously adapting to the evolving landscape of health tech. By tackling these issues head-on, we can ensure that health tech serves its intended purpose of improving health outcomes while upholding the fundamental right to privacy and respecting the ethical principles of healthcare.

5. CONCLUSION

Maintaining confidentiality in the health tech space presents significant legal and ethical challenges. With the increasing use of technology in healthcare, it is essential to strike a delicate balance between using patient data for research and innovation while ensuring individual privacy is respected. This study has explored various aspects of confidentiality in health tech, including legal obligations, ethical considerations, and the potential challenges that may arise. Healthcare providers and health tech companies must comply with laws and regulations on confidentiality, such as the Nigerian Data Protection Act, Code on Medical Ethics in Nigeria (Rules of Professional Conduct for Medical and Dental Practitioners), National Health Act, among others. These laws outline the requirements for protecting patient data and define the rights and responsibilities of both patients and healthcare organisations. Adhering to these legal obligations is crucial for avoiding legal repercussions and maintaining patient trust.

The dynamic nature of technology and the ever-evolving threat landscape necessitate a constant review and enhancement of data privacy practices. Regular audits and assessments can help identify vulnerabilities, ensuring that health tech companies and healthcare providers stay ahead of potential breaches. Collaboration within the industry and with regulatory bodies is essential to establish consensus on ethical guidelines and best practices for maintaining confidentiality. Maintaining confidentiality in the health tech space is a complex task that requires a comprehensive approach. It involves navigating legal obligations, addressing ethical considerations and implementing robust security measures. By doing so, health tech companies and healthcare providers can ensure the protection of patient data while promoting research and innovation in the health tech space.

---

[46] F.F. Ozair et al., 'Ethical Issues in Electronic Health Records: A General Overview' *Perspect Clin Res.* (2015) 6 (2) 73-76.

6. RECOMMENDATIONS

The following recommendations will go a long way in addressing the challenges of maintaining confidentiality in health tech:

1. *Implement Robust Data Security Measures*: Health tech companies should invest in state-of-the-art data security measures, such as encryption, secure storage, and access controls, to protect patient data from unauthorised access and breaches.
2. *Develop Comprehensive Privacy Policies*: A clear and comprehensive privacy policy should outline how patient data is collected, used, stored, and shared. This policy should align with legal requirements, ethical standards, and best practices.
3. *Prioritise Data Anonymisation and De-identification*: Health tech companies should prioritise the anonymisation and de-identification of patient data to protect individual privacy. This can involve removing or encrypting identifiable information, as well as aggregating data for analysis.
4. *Establish Training Programs on Confidentiality*: Healthcare providers and health tech companies should educate their employees on the importance of maintaining patient confidentiality. Such training programs should cover ethical guidelines, legal obligations, and proper data handling practices.
5. *Ensure Transparency and Informed Consent*: Transparency is crucial in maintaining patient trust. Health tech companies should provide clear information about data usage practices, risks, and benefits to patients and obtain their informed consent before collecting or sharing their data.
6. *Regularly Audit and Assess Data Privacy Practices*: Conducting regular audits and assessments of data privacy practices can help identify any vulnerabilities or lapses in security. This allows for timely remediation and continuous improvement in maintaining confidentiality.
7. *Ensure Collaboration Between Stakeholders*: Collaboration between health tech companies, healthcare providers, researchers, and regulatory bodies can help establish consensus on ethical standards and guidelines for maintaining confidentiality in health tech. These collaborations can lead to industry-wide best practices and standards that prioritise patient privacy.