Ethical and legal implications of doctor–patient confidentiality in the age of technological advancements: Ensuring privacy and trust in healthcare services

Mlondolozi Mvikweni[1]

Abstract

In the contemporary digital age, the traditional principles of doctor–patient confidentiality face increasing challenges due to rapid technological advancements. This research explores the ethical and legal implications of maintaining confidentiality in healthcare, specifically focusing on electronic health records (EHRs), telemedicine and the burgeoning use of big data. It critically examines the ways in which these technologies, while possibly enhancing the efficiency of healthcare delivery, also introduce substantial risks to patient privacy and trust. The study analyses South African constitutional provisions alongside relevant international conventions and legislative frameworks that govern the right to privacy. This includes a detailed evaluation of cybersecurity measures and the ethical guidelines necessary to navigate these challenges. Through a comprehensive review of the case law and statutory obligations, this research provides strategies for healthcare providers to uphold confidentiality, ensure informed consent and balance the benefits of technological innovation against the imperative to protect sensitive patient information. Furthermore, a comparative analysis of the South African healthcare system and the Cuban healthcare system is presented to offer a broader perspective on maintaining doctor–patient confidentiality in diverse socio-economic contexts.

Keywords: confidentiality, patient autonomy, cybersecurity, telemedicine, international conventions, electronic health records, EHR, Fourth Industrial Revolution, 4IR

[1] Walter Sisulu University. Email: 221182802@mywsu.ac.za

https://doi.org/10.47348/IJAR/2025/a2

1. Introduction

Doctor–patient confidentiality is a cornerstone of a healthcare system, providing as it does an ethical and legal framework that protects patient privacy, fosters trust and facilitates the open communication necessary for effective medical care (Hiller & Zettler, 2019). The moral justification for maintaining discretion and confidentiality in the medical profession stems from the rights that emerge from the trust-based interactions between doctors and patients, and society at large (Freckelton, 2013). As noted by Al-Amarat (2011), patients' willingness to disclose sensitive information is contingent upon the assurance that such information will be protected from unauthorised access. However, the proliferation of technological advancements such as electronic health records (EHRs), telemedicine and big data analytics has introduced unprecedented challenges to this fundamental principle (Ismail & Kinchin, 2019). The advent of the Fourth Industrial Revolution (4IR) and its associated technologies necessitates a thorough re-evaluation of the existing ethical and legal frameworks that govern doctor–patient relationships.

In South Africa, the constitutional right to privacy, as enshrined in section 14 of the Constitution of the Republic of South Africa, 1996, provides a fundamental legal basis for doctor–patient confidentiality. This right is further augmented by the National Health Act 61 of 2003 (NHA), which articulates specific provisions for the protection of patient information. Section 14 of the NHA mandates that patient information should not be disclosed without a patient's consent, except in specific circumstances, such as public interest or legal obligations. The Protection of Personal Information Act 4 of 2013 (POPIA) strengthens this further by regulating the way in which personal data, including medical records, are processed, ensuring that patient information is kept secure and confidential.

The case of *Jansen van Vuuren & Another NNO v Kruger*[2] established the legal duty of physicians to respect patient confidentiality under the common law, underscoring the fact that this duty is not merely an ethical matter but also legally enforceable. This ruling highlights the Judiciary's recognition of the importance of maintaining patient privacy in South Africa.

Despite these protections, the increasing reliance on digital healthcare solutions has introduced significant vulnerabilities. The digitisation of medical records, while enhancing efficiency and accessibility, also raises the risk of data breaches, unauthorised access and the misuse of patient information (Goodman, 2015). Telemedicine, which enables remote consultations and monitoring, introduces

[2] 1993 (4) SA 842 (A).

https://doi.org/10.47348/IJAR/2025/a2

additional layers of complexity in ensuring confidentiality, particularly regarding the security of communication channels and the integrity of data transmission (Alpay, 2019). As healthcare systems increasingly rely on cloud storage and third-party service-providers, patient data risk possibly being exposed to a broader range of threats, necessitating robust cybersecurity measures and clear legal guidelines (Price & Cohen, 2019).

This study aimed to analyse the ethical and legal dimensions of doctor–patient confidentiality in the context of these technological advancements, identifying gaps in existing legal and ethical frameworks and proposing strategies to enhance patient privacy and trust in healthcare services. By examining the legal obligations to maintain confidentiality, analysing the challenges posed by digital healthcare technologies and exploring the role of ethics and trust, this research set out to inform policymakers, healthcare providers and legal professionals, in so doing facilitating the development of robust frameworks that balance privacy protection against effective healthcare delivery in the digital age.

2. Research problem

In modern healthcare systems, doctor–patient confidentiality stands as a cornerstone principle, one that safeguards patient privacy and fosters trust in the medical relationship. The problem lies in the complexity and ambiguity surrounding doctor–patient confidentiality laws, which may lead to inconsistencies in practice, breaches of privacy and the erosion of patient trust. Emerging challenges such as electronic health records, telemedicine and data sharing among healthcare providers raise critical questions regarding the scope, limitations and enforcement of confidentiality provisions.

Technological advancements necessitate a consistent examination of confidentiality laws to ensure their alignment with contemporary healthcare realities and patient expectations of their ethical performance. The digital age calls for a robust evaluation of existing frameworks to balance privacy protection against effective healthcare delivery. This research aimed to respond to these matters by examining the ethical and legal dimensions of doctor–patient confidentiality in the 4IR, identifying gaps in legal and ethical frameworks and promoting enhanced standards in medical practice.

Moreover, the case of *Minister of Health & Another v Goliath & Others*[3] emphasises the growing need for clarity and the consistent application of confidentiality principles in the context of technological

[3] 2014 (2) SA 586 (CC).

advancements. This case illustrates the Judiciary's engagement with the complexities of balancing patient rights and public health concerns in the digital era.

3. Research questions

To respond to the research problem comprehensively, the following questions guided this study:

1. What are the legal obligations for maintaining doctor–patient confidentiality in the context of technological advancements in South Africa?
2. How do South African healthcare providers balance the need for technological innovation with the legal and ethical obligations to protect patient confidentiality?
3. What specific measures can be implemented to enhance cybersecurity and data protection in digital healthcare environments to safeguard patient information?
4. How do different international jurisdictions, such as Cuba, approach the balance between leveraging technology in healthcare and protecting doctor–patient confidentiality, and what lessons can South Africa learn from these experiences?

4. Study objectives

This study aimed to achieve the following objectives:

1. To analyse the legal framework governing doctor–patient confidentiality in South Africa, including key legislation such as the NHA and POPIA, and the way these laws are applied in the digital age.
2. To assess the challenges and risks posed by technological advancements in healthcare, such as electronic health records and telemedicine, to the protection of patient confidentiality.
3. To examine the ethical considerations and dilemmas faced by healthcare providers in balancing technological innovation with patient privacy and trust.
4. To identify and evaluate strategies for enhancing cybersecurity and data-protection measures in digital healthcare environments.
5. To compare the approaches to doctor–patient confidentiality in South Africa and other selected international jurisdictions, such as Cuba, to draw lessons and best practices from them.

https://doi.org/10.47348/IJAR/2025/a2

5. Study rationale

This study was informed by the increasing importance of doctor–patient confidentiality in the digital age. The researcher's own experiences and observations highlight the necessity for clear legal and ethical frameworks that respond to the challenges posed by technological advancements in healthcare. There are limited specific laws in South Africa that speak directly to doctor–patient confidentiality in the digital age; therefore, the study was grounded in legal and ethical perspectives. This study analysed the legislative framework and ethical considerations of doctor–patient confidentiality in the digital age and provides recommendations on how the challenges can be overcome.

6. Significance of the study

This study considered the protection of patient privacy in the context of digital healthcare by investigating the relevant legal issues and perspectives. It should be of benefit to stakeholders such as patients, healthcare providers, lawmakers and educators by aiming to improve privacy, trust and compliance. Informed decisions regarding the use of technology in healthcare and the associated confidentiality implications are critical to patients, healthcare providers and legal professionals. This study set out to fill gaps in the existing research by providing an up-to-date analysis of the legal perspectives on doctor–patient confidentiality in the digital age. The study also offers practical recommendations for healthcare providers to enhance their data-protection protocols, ensuring compliance with legal requirements and fostering a culture of confidentiality. In addition, the findings of this research may inform the development of new policies and guidelines in the healthcare sector, as a result promoting a more robust and ethical approach to managing patient information in the digital era.

7. Literature review

The existing literature emphasises both the importance and the challenges of maintaining doctor–patient confidentiality in the face of technological advancements. Studies by Dehling and Sunyaev (2017) stress the fundamental requirements of information technology security, including confidentiality, integrity and availability. These authors assert that restricting access to information to only those who are authorised to have access to it is critical to maintaining confidentiality in healthcare settings.

The ethical implications of confidentiality have been widely discussed in the literature. Freckelton (2013) notes that the traditional duty of confidentiality has been significantly adjusted to permit, and

sometimes require, practitioners to disclose information to support the health and safety of patients, third parties and the broader community. This shift raises complex ethical questions about balancing individual patient rights against public health interests.

Allard et al (2019) argue that while laws and ethical guidelines exist to protect patient information, emerging challenges such as electronic health records, telemedicine and data-sharing among healthcare providers raise critical questions about the scope, limitations and enforcement of confidentiality provisions. They call for a consistent examination of confidentiality laws to ensure their alignment with contemporary healthcare realities and patient expectations.

Moreover, comparative studies provide insights into the ways in which different countries approach the issue of doctor–patient confidentiality in the digital age. For example, a study by Batha and Lilly (2014) examined the legal and ethical frameworks governing patient privacy in the European Union; it highlighted the importance of the EU's General Data Protection Regulation (GDPR) in setting standards for data protection.

8. Legal framework governing doctor–patient confidentiality in South Africa

The legal framework governing doctor–patient confidentiality in South Africa is primarily the Constitution, the NHA and POPIA.

Section 14 of the Constitution of the Republic of South Africa, 1996, guarantees the right to privacy, which is a fundamental right that extends to the protection of personal health information. This provides a broad foundation for upholding patient confidentiality in the digital age. It ensures that individuals have the right to control the dissemination of information about their health and medical conditions.

As highlighted by Currie and De Waal (2013), the right to privacy under the Constitution is not absolute but can be limited in certain circumstances, such as when there is a legitimate public interest or a legal obligation to disclose information. Any limitation on the right to privacy must be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom (Currie & De Waal, 2013).

The NHA provides specific guidelines for maintaining patient confidentiality in the healthcare context. Section 14 of the Act prohibits the unauthorised disclosure of patient information, except in circumstances where consent is obtained or where disclosure is required by law or the public interest. This provision is crucial to

https://doi.org/10.47348/IJAR/2025/a2

ensuring that healthcare providers respect patient privacy in their day-to-day practices.

The NHA also stipulates that patient information should be used only for purposes related to their medical care and treatment, unless there is a valid reason for using it otherwise. According to Dhai and McQuoid-Mason (2011), this restriction is essential to building trust between patients and healthcare providers.

The NHA also outlines exceptions to the rule on confidentiality. These exceptions balance individual rights against the need to protect broader societal interests. Patient information may be disclosed without consent when required by law, such as reporting communicable diseases to public health authorities. This enables public health surveillance and ensures the containment of outbreaks. Disclosure may also be required when it is in the public interest, such as when preventing imminent harm to a patient or others. When a patient is a minor, disclosure to their parent may be required, or prescribed by order of a court. In such cases, healthcare providers must exercise sound judgement and adhere to ethical guidelines to minimise the impact on patient privacy.

POPIA, which came into full effect on 1 July 2021, regulates the processing of personal information, including health data, by both public and private entities. The Act sets out specific conditions for the lawful processing of personal information, including obtaining consent, ensuring data security and providing transparency to data subjects.

In addition to these primary pieces of legislation, the Health Professions Council of South Africa (HPCSA) provides ethical guidelines and professional standards for healthcare practitioners, emphasising the importance of maintaining patient confidentiality (HPCSA, 2016). The HPCSA's ethical rules outline the obligations of healthcare professionals to protect patient information; more specifically, they provide guidance on how to handle sensitive data in various healthcare settings.

The case of *Minister of Health & Another v Treatment Action Campaign*[4] underscores the importance of balancing patient rights and public health concerns. This case, which involved the provision of antiretroviral drugs to pregnant women, highlights the ethical dilemmas faced by healthcare providers when protecting patient confidentiality while dealing with broader public health objectives.

[4] 2002 (5) SA 721 (CC).

https://doi.org/10.47348/IJAR/2025/a2

9. Challenges and risks posed by technological advancements

Technological advancements in healthcare have introduced new challenges and risks to the protection of patient confidentiality, in particular in the case of EHRs, telemedicine, data-sharing and interoperability, mobile health (mHealth) and cloud computing. These are outlined below.

EHRs: Whereas EHRs offer numerous benefits, such as the improved efficiency, accessibility and coordination of care, they also increase the risk of data breaches and unauthorised access (Buntin et al, 2010). Security vulnerabilities in EHR systems can expose sensitive patient information to cyberattacks, which could possibly lead to identity theft, fraud and reputational damage.

Telemedicine: Telemedicine, which involves the delivery of healthcare services remotely through technology, raises concerns about the security and privacy of communication channels (Alpay, 2019). In particular, the transmission of sensitive patient information over unsecured networks can increase the risk of interception and unauthorised access.

Data-sharing and interoperability: The sharing of patient data among healthcare providers and institutions, while necessary for co-ordinated care, increases the potential for privacy breaches. Interoperability standards, which facilitate the exchange of data across different systems, also create new attack surfaces for cybercriminals (Vestal, 2016).

Mobile health (mHealth): The use of mobile devices and apps for healthcare purposes raises concerns about the security and privacy of patient data stored on these devices. Mobile devices are often less secure than traditional desktop computers and may be vulnerable to malware, hacking and physical theft (Kumar et al, 2013).

Cloud computing: The use of cloud computing services for storing and processing patient data raises concerns about data security and jurisdictional issues. Cloud providers may be subject to different legal and regulatory requirements, which could possibly affect the protection of patient information (Kruse et al, 2017).

10. Ethical considerations and dilemmas

Healthcare providers face numerous ethical dilemmas in balancing technological innovation against patient privacy and trust. These dilemmas include matters of informed consent, data ownership and control, transparency and accountability, and beneficence and non-maleficence:

https://doi.org/10.47348/IJAR/2025/a2

Informed consent: Obtaining informed consent from patients for the use of their data in digital healthcare systems can be challenging. For one thing, patients may not fully understand the risks and benefits of data-sharing and may feel pressured to consent to certain practices.

Data ownership and control: Determining who owns and controls patient data in digital healthcare environments is a complex ethical issue. Patients may have limited control over the way their data are used and shared by healthcare providers and third-party organisations.

Transparency and accountability: Ensuring transparency and accountability in the use of patient data is critical to maintaining trust. Healthcare providers need to be transparent about their data practices and accountable for any breaches of confidentiality.

Beneficence and non-maleficence: Healthcare providers must balance the potential benefits of using technology to improve patient care against the risks of harm to patient privacy. The principle of beneficence requires healthcare providers to act in the best interests of their patients, while the principle of non-maleficence requires them to avoid causing harm (Beauchamp & Childress, 2019).

11. Strategies for enhancing cybersecurity and data protection

To respond to the challenges and risks posed by technological advancements, healthcare providers could implement a range of strategies to enhance cybersecurity and data protection. These strategies could include:

Data encryption: Encrypting sensitive patient data, both in transit and at rest, is essential to protecting it from unauthorised access. Moreover, encryption algorithms should be updated regularly to reflect current security standards (NIST, 2018).

Access controls: Implementing strict access controls, such as role-based access control (RBAC) and multi-factor authentication (MFA), can limit who has access to patient data and reduce the risk of insider threats.

Network security: Securing healthcare networks with firewalls, intrusion detection systems, and virtual private networks (VPNs) can help to prevent unauthorised access to patient data by external sources.

Data-loss prevention (DLP): Implementing DLP solutions can help to prevent the unauthorised exfiltration of sensitive data from healthcare networks.

Security awareness training: Providing regular security awareness training to healthcare staff can help to reduce the risk of human error and social engineering attacks.

https://doi.org/10.47348/IJAR/2025/a2

Incident response planning: Developing and implementing incident response plans can help healthcare organisations to respond quickly and effectively to data breaches and other security incidents.

Regular security audits: Conducting regular security audits and vulnerability assessments can help to identify and deal with potential weaknesses in healthcare IT systems.

12. Comparative analysis: South Africa vs Cuba

To offer a broader perspective on maintaining doctor–patient confidentiality in diverse socio-economic contexts, this section presents a comparative analysis between the South African healthcare system and its Cuban equivalent.

The South African healthcare system is characterised by a dual structure: a well-developed private sector that serves a minority of the population and a resource-constrained public sector serving the majority (Ataguba & McIntyre, 2011). This dual structure creates inequalities in access to care and disparities in data-protection capabilities.

The Cuban healthcare system, in contrast, is characterised by universal access, a focus on preventive care and a highly integrated and centralised structure (Kirk, 2010). Cuba's emphasis on public health and social solidarity has led to innovative approaches to managing patient data while maintaining patient confidentiality.

Key differences in the approaches to doctor–patient confidentiality in South Africa and Cuba include data governance, technology infrastructure and a privacy culture. Each of these is now considered in turn.

12.1 Data governance

South Africa relies on a combination of legislation and ethical guidelines to govern data protection, whereas Cuba has a more centralised and state-controlled approach. South Africa and Cuba also have distinct approaches to data governance due to their differing political and regulatory environments. For instance, in South Africa, data protection is primarily governed by POPIA, which is aligned with international standards such as the General Data Protection Regulation (GDPR) in Europe. POPIA establishes rules for data processing, storage and security, ensuring that organisations are held accountable for data breaches. In addition, ethical guidelines provided by institutions such as the National Health Research Ethics Council (NHREC) play a significant role in regulating data use in the healthcare sector. However, despite these legal and ethical frameworks, enforcing data-privacy laws remains a challenge, particularly with the increasing number of cyber threats.

https://doi.org/10.47348/IJAR/2025/a2

In contrast, Cuba follows a centralised state-controlled approach to data governance in which the government regulates the collection and use of personal data. Patient data are managed almost exclusively by the state-run healthcare system, ensuring uniformity and standardisation but also limiting individual autonomy over personal information. Unlike South Africa, Cuba has less transparency regarding data-security policies because the government retains control over most of the digital infrastructure. Ethical guidelines in Cuba prioritise collective well-being over individual privacy rights, which reflects the socialist emphasis on societal benefit rather than private control.

12.2 Technology infrastructure

South Africa's reliance on digital healthcare technologies is growing, but disparities in access to technology and cybersecurity resources continue to exist. Cuba has made significant investments in telemedicine and health informatics but faces challenges related to limited access to technology and connectivity. Both countries have made notable investments in digital healthcare, but they face unique challenges due to disparities in access to technology and resources. In South Africa, the adoption of digital healthcare technologies such as electronic health records, mHealth applications and AI-driven diagnostics is gaining momentum. However, the country still experiences significant disparities in access to these technologies, particularly in rural and under-resourced healthcare facilities that often lack reliable internet connectivity, information technology (IT) infrastructure and adequate cybersecurity measures. In addition, cybersecurity threats, including ransomware attacks on public health institutions, are becoming a growing concern. Although efforts are being made to integrate e-health systems across the public and private sectors, ensuring interoperability between different systems remains a significant challenge.

Cuba, in contrast, has made substantial progress in telemedicine and health informatics, despite its limited access to global digital resources. The country has developed national-level health informatics systems that focus on preventive care and efficient resource allocation. However, restricted internet access and outdated hardware limit the full potential of these advancements. Unlike South Africa, where private-sector involvement drives digital healthcare innovations, Cuba's state-driven approach has resulted in a reliance on domestically developed software solutions. While this limits exposure to international cybersecurity threats, it also restricts technological advancements owing to resource constraints and a lack of access to global innovations.

https://doi.org/10.47348/IJAR/2025/a2

12.3 Privacy culture

In South Africa, a culture of privacy awareness is evolving, driven by the implementation of POPIA and growing public concern about data breaches. Cuba has a longstanding tradition of protecting patient information that is rooted in socialist values of social solidarity and collective responsibility.

The approach to data privacy in South Africa and Cuba is influenced by legal, ethical and cultural factors. In South Africa, a culture of privacy awareness is steadily evolving, driven by the implementation of POPIA and an increasing number of high-profile data breaches. Both the public and the private sectors are becoming more conscious of data security, particularly as concerns about government surveillance and corporate misuse of personal information grow. In addition, debates about balancing privacy rights against public health needs, such as during pandemics, have become more pronounced. However, the degree of trust in institutions that handle personal data varies, with scepticism existing towards both government and private organisations' ability to protect sensitive information.

Cuba, in contrast, has a longstanding tradition of protecting patient information in its state-run healthcare system, but with a strong emphasis on collective responsibility rather than individual rights. Unlike South Africa, where legal frameworks actively shape data privacy, Cuba's approach is deeply rooted in socialist values that prioritise the well-being of society over individual data autonomy. As a result, there is less public discourse on privacy rights, as government policies largely dictate data-management practices. In addition, the culture of social solidarity means that citizens are generally more accepting of sharing their health data in support of public health initiatives such as national vaccination programmes.

13. Recommendations

Based on the findings of this study, the following actionable recommendations are made to enhance doctor–patient confidentiality in the digital age. These are aimed at fortifying legal safeguards, improving governance, enhancing the technological infrastructure, increasing patient awareness and fostering international collaboration – and ultimately bolstering trust in healthcare services.

First, amend existing laws and regulations to respond to the specific challenges posed by digital healthcare technologies. This entails undertaking a comprehensive review of the NHA, POPIA and related statutes to incorporate explicit provisions for data protection, breach notification and accountability in digital contexts. Legislation should reflect updated definitions of 'health information' to include

https://doi.org/10.47348/IJAR/2025/a2

all digital formats and ensure that the penalties for violations are stringent enough to deter misconduct.

Second, establish clear data-governance structures and promote ethical data-stewardship practices in healthcare organisations. These should include the creation of dedicated data-protection officers or committees responsible for overseeing compliance with privacy laws, developing internal data-governance policies and conducting regular risk assessments. The implementation of data-minimisation principles, where only necessary data are collected and retained, is crucial.

Third, increase investment in robust cybersecurity infrastructure and comprehensive training for healthcare providers. This should encompass adopting advanced encryption technologies, implementing multi-factor authentication and employing real-time threat-detection systems. Regular cybersecurity training for all healthcare staff is vital to dealing with human error, which remains a significant source of data breaches.

Fourth, develop patient education initiatives to raise awareness of their rights and responsibilities regarding data privacy in digital healthcare settings. This includes creating user-friendly materials which explain how patient data are collected, used and protected, and the rights patients have to access, correct and control their information. Promoting transparency and open communication is crucial to building trust.

Finally, participate actively in international collaborations to share best practices and develop common standards for data protection in healthcare. This should involve engaging with international organisations such as the World Health Organization (WHO), the European Union and other global bodies to align with international benchmarks for data privacy and security. Exploring comparative studies, such as the referenced comparison with the Cuban healthcare system, and learning from different approaches and solutions that can be adapted to the local South African context are also important steps that should be taken.

14. Conclusion

In conclusion, doctor–patient confidentiality remains a cornerstone of ethical medical practice, but it faces significant challenges in the face of rapid technological advancements. Maintaining trust in healthcare services necessitates a balanced approach, one in which healthcare providers must adeptly navigate complex ethical dilemmas while adhering strictly to legal frameworks. This research underscores the critical importance of proactively safeguarding patient data in digital environments.

https://doi.org/10.47348/IJAR/2025/a2

The integration of technology into healthcare has revolutionised data management, but it has simultaneously introduced vulnerabilities and amplified existing risks. Cases such as *Jansen van Vuuren & Another NNO v Kruger*, in which the duty to respect patient confidentiality was affirmed as a legal duty, highlight the courts' emphasis on protecting patient privacy. The evolving digital landscape requires that ethical considerations and legal safeguards be adapted accordingly to guarantee continuing respect for patients' rights.

The recommendations provided in this article offer a roadmap for strengthening data-protection measures, improving compliance and fostering a culture of trust. They include enhancing legal and regulatory frameworks, promoting data governance and stewardship, investing in cybersecurity infrastructure, enhancing patient education and fostering international collaboration. Moreover, it recognises the necessity of ongoing vigilance and adaptation in response to emerging threats and technological developments.

Ultimately, the imperative to protect doctor–patient confidentiality in the age of technological advancements transcends mere compliance with legal mandates. It is a moral and ethical obligation to uphold patient autonomy, maintain trust and ensure that individuals feel secure when seeking medical care. By implementing the recommendations presented in this research, healthcare providers, policymakers and legal professionals can work together to promote a more robust and ethical approach to managing patient information, ensuring the long-term sustainability and integrity of the healthcare system. Through collective effort and a commitment to ethical practices, South Africa will be able to navigate the complexities of digital healthcare while upholding the fundamental right to privacy.

References

Al-Amarat, MS 'The classroom problems faced teachers at the public schools in Tafila Province, and proposed solutions' (2011) 3(1) *International Journal of Educational Sciences* 37–48.

Allard, A, Anciaux, N, Bouganim, L, Guo, Y, Folgoc, L & Nguyen, BC 'Secure personal data servers: a vision paper' (2019) 12(12) *Proceedings of the VLDB Endowment 2001–2014*.

Alpay, LL 'Legal and ethical aspects of telemedicine' (2019) 25(3) *Journal of Telemedicine and Telecare* 131–138.

Ataguba, JE & McIntyre, D 'The benefit incidence of health care spending in South Africa' (2011) 1(1) *Health Economics Review* 1–13.

Batha, K & Lilly, M 'The EU data protection directive: What US organizations need to know' (2014) 16(5) *Journal of Health Care Compliance* 45–49.

Beauchamp, TL & Childress, JF *Principles of biomedical ethics* 8 ed (Oxford University Press 2019).

https://doi.org/10.47348/IJAR/2025/a2

Buntin, MB, Burke, MF, Hoaglin, MC & Blumenthal, D 'The benefits of health information technology: A review of the recent literature shows predominantly positive results' (2010) 29(3) *Health Affairs* 464–471.

Castro, J 'E-governance and data protection in Cuba: A state-controlled model' (2020) 12(3) *Global Policy Review* 78–92.

Currie, I & De Waal, J *The Bill of Rights handbook* 6 ed (Juta & Co 2013).

Data Privacy Africa *The state of cybersecurity and data protection in South Africa* (2022), available at https://www.dataprivacyafrica.org

Dehling, T & Sunyaev, A 'Information technology security in healthcare: A systematic review and meta-analysis' (2017) 24(5) *Journal of the American Medical Informatics Association* 906–920.

Densham, P & Wilkinson, M 'Data protection and privacy in South Africa: The implementation of POPIA in a digital economy' (2021) 65(2) *Journal of African Law* 245–263.

Dhai, A & McQuoid-Mason, D *Bioethics for healthcare professionals* (Juta & Co 2011).

Freckelton, I 'Doctors' duty of confidentiality: Legal and ethical change' (2013) 20(4) *Journal of Law and Medicine* 828.

Goodman, KW 'Ethics, computing, and medicine: Informationalism and the moral fabric of healthcare' (2015) 24(3) *Cambridge Quarterly of Healthcare Ethics* 306–315.

Government of Cuba. *Decree-Law No 370 on Informatization of Society*, available at https://www.gacetaoficial.gob.cu

Government of South Africa. *Protection of Personal Information Act (POPIA), Act No 4 of 2013*, available at https://www.justice.gov.za

Health Professions Council of South Africa (HPCSA) *Booklet 1: General ethical guidelines for health care professions* (HPCSA 2016).

Hiller, TJ & Zettler, PJ 'Information privacy under siege' (2019) 381(13) *New England Journal of Medicine* 1185–1187.

Kirk, JM *Medical care, education, and welfare services in Cuba* (Centre for Global Education 2010).

Kumar, S, Nilsen, W, Abernethy, A, Atienza, A, Patrick, K, Pavel, M, Riley, WT, Shar, A, Spring, B & Spruijt-Metz, D 'Mobile health technology for better health' (2013) 68(5) *American Psychologist* 276.

Makulilo, AB *Data protection in Africa: A comparative analysis of South Africa and other jurisdictions* (Springer 2016).

Martínez Pérez, G & Torralba Rodríguez, S 'Telemedicine in Cuba: Achievements and challenges in a centralized healthcare system' (2020) 29(1) *Cuban Journal of Health Informatics* 50–67.

National Health Research Ethics Council (NHREC) *Ethical guidelines for health research in South Africa* (NHREC nd), available at https://www.nhrec.org.za

National Institute of Standards and Technology (NIST) *Framework for improving critical infrastructure cybersecurity* (NIST 2018).

Price, WN II & Cohen, IG 'Privacy in the age of medical big data' (2019) 25(1) *Nature Medicine* 37–43.

Valdés, R 'Health informatics in Cuba: A socialist approach to digital health' (2019) 34(4) *Latin American Journal of Public Health* 112–130.

Vestal, W 'Interoperability and population health: What's the connection?' (2016) 70(5) *Healthcare Financial Management* 48–54.

World Health Organization (WHO) *Digital health strategies in low- and middle-income countries: The case of South Africa and Cuba* (WHO 2021), available at https://www.who.int

Legislation

Constitution of the Republic of South Africa, 1996

National Health Act 61 of 2003

Protection of Personal Information Act 4 of 2013 (POPIA)

Cases

Jansen van Vuuren & Another NNO v Kruger 1993 (4) SA 842 (A)

Minister of Health & Another v Goliath & Others 2014 (2) SA 586 (CC)

Minister of Health & Another v Treatment Action Campaign 2002 (5) SA 721 (CC)

https://doi.org/10.47348/IJAR/2025/a2